NATIONAL DEFENSE INDUSTRIAL ASSOCIATION

STRENGTH THROUGH INDUSTRY & TECHNOLOGY

JUNE 1998

14th ANNUAL NDIA SYMPOSIUM & EXHIBITION ON SECURITY TECHNOLOGY

Approved for Public Release. Distribution is unlimited

14th Annual Security Technology

Table of Contents

Session 1: Threat Environment and the Worldwide Context

Session 2: Planning to Meet the Threat

Session 3: Weapons of Mass Destruction: Protection and Response

Session 4: Technical and Policy Focus Group

Group A:

Group B:

Group C:

Session 5: Addressing Our Domestic Vulnerabilities

Session 6A: A DoD Force Protection

Session 6B: DoD PSEAG Programs

Session 7: Transportation Security

Session 8A: Physical Security Technologies

Session 8B: Physical Security Technologies

Session 9: Information Protection Technologies

Several presentations and papers were not provided to DTIC by 29 July 1998. If submitted to DTIC after this date, they will be available electronically at the following Internet address: http://www.dtic.mil/stinet/security

Presentations not received in time for inclusion are:

Kenneth Piernick, FBI - "The Domestic Threat"
Jeffrey David, OST - "A Model for Requirements Definition - The National Research and Development Program for Combating Terrorism"
Dr. Gary Resnick, U.S. Army CBDCOM, APG
Edward Sueter - "Mistakes to Avoid During Bomb Incident Planning"
Robert Kelley, Orbital Science Corporation
William Keely, DISA - "Defense Megacenter Information Security"
Roger Calahan, NationsBanc

Opening Remarks

Brigadier General Roger C. Smith, USAF (Ret.)
Chairman, Security Division

Welcome to the 14th Annual Symposium and Exhibition on Security Technology.

I am Roger Smith, Chairman of the NDIA Security Division.

Many thing have changed in the fourteen years since our first symposium in 1984 -- not the least of which has been the evolution of our sponsoring association.

The merger, one year ago, of the American Defense Preparedness Association and the National Security Industrial Association has resulted in more than a larger, stronger National Defense Industrial Association.

By combining into a new association with more than nine hundred company members and 28,000 individual members, NDIA has capitalized on the strengths of both prior associations and is now recognized as the premier association serving the entire spectrum of the defense and national industrial base.

On behalf of the Association, I welcome each of you. We hope this symposium, which has always been one of our most productive and successful events, will again this year provide productive opportunities for the open exchange of views and the sharing of information.

This is especially important in view of new concerns and directions in the security and protection environment.

I'm pleased now to introduce our 1998 Symposium Chair, Dr. Paula Scalingi , director of the new Infrastructure Assurance Center at Argonne National Laboratory. She has had a key role in developing our agenda and in assembling a truly impressive slate of guest speakers.

Symposium Purpose and Overview

Dr. Paula Scalingi
Director, Infrastructure Assurance Center
Argonne National Laboratory

In this, our fourteenth annual NDIA Security Symposium, we will be addressing all aspects of the new dimensions in security threats and countermeasures, providing new insights and perspectives into an evolving world situation.

Both at home and abroad the United States and its international partners are facing threats ever more serious to the individual and to military and domestic resources. The evolution from a bi-polar world to one dominated by less-easily defined and significantly less-predictable adversaries is overlaid upon fundamental societal changes throughout the world and exponential advances in technology.

This symposium will focus upon these new dimensions of the security and protection envelope; both its continuing expansion driven by a more diverse threat, and the potentially unbounded opportunity that new technology provides.

We will highlight topics central to this theme, including specific threats and the operational environment with which both military and domestic agencies must contend; government and industry initiatives to address these challenges; current and future technologies in both the physical and information-based world; the threat of weapons of mass destruction and planning for response; and the future of national budgets and resource availability.

We hope this symposium will be interesting and productive, and that you will contribute to a lively interchange as we address one of our most critical and pressing problems.

Stevan D. Mitchell
Keynote Remarks

From PCCIP to PDD:
First Steps in Infrastructure Assurance

National Defense Industrial Association
14th Annual Security Technology Symposium and Exhibition
"New Dimensions in Security Threats and Countermeasures"
June 15-18, 1998

[Slide 1: PCCIP to PDD]

Good morning. As if there were ever any doubt, let me first make clear that I have done very little *personally* to merit appearing before you here today--particularly nothing so grand as to merit my being permitted to make these opening remarks. I am here as a messenger for and representative of a new, novel and needed government *capability*. It is this capability that merits a position of distinction in your program, as well as your time, attention and continuing support. I will take a few minutes to introduce you to this new capability, place it in recent historical context, and describe it alongside other features of PDD-63 and the initiative that the President announced on May 22, 1998 at the Naval Academy Graduation in Annapolis.

Dr. Jeffrey Hunker, the newly-named Director of the Critical Infrastructure Assurance office, regrets that he could not be here to talk to you about the office and other important aspects of the Administration's Critical Infrastructure Assurance initiative. But he is not only in the middle of doing all that is required in order to stand up a new government *office*, like testifying before Congress and negotiating budgets with cabinet secretaries. He is trying to do what is required to stand up a new government *capability* where none has previously existed.

The Critical Infrastructure Assurance Office is, quite literally, a new government capability residing right at the point where our national security and economic security merge. It is an office of the Department of Commerce that provides support to the National Security Council. It is an office that assists an ambitious interagency effort involving over 20 federal agencies and White House offices, an effort that will influence how all federal government agencies do business. It is an office that has the responsibility to coordinate its activities with White House offices as diverse as the National Economic Council, National Security Council, the Office of Management and Budget, and the Office of Science and Technology Policy. It is the living embodiment of the challenge of infrastructure assurance—with obligations to both the public and private sectors, and a duty to defend both national and economic security.

[Slide 2: Three Events]

Before I go on for too long about how difficult *our* job is going to be, let me take you back through some very recent history to describe how the federal government's efforts to protect the critical infrastructures took on its unique and multiple forms. I will describe three significant events: Executive Order 13010, the Final Report of the President's Commission on Critical Infrastructure Protection, and Presidential Decision Directive 63, addressing Critical Infrastructure Protection.

The Federal Government's newfound "infrastructure awareness" has come about through the persistence of key people across government, catalyzed by tragic events that reminded us that terrorism really can happen here, too. Events like the World Trade Center and Oklahoma City bombings and the Tokyo subway attack remind us that there are, "out there," those with the will to do harm to our people and our way of life. They are out there. That is now a given. We will not always be able to predict with certainty exactly who they are, who will act next, nor against whom they will act. We will not always sympathize with, understand or even know their motives. We must also accept that some of them may be our very own citizens. And so our defense must be predicated upon their capabilities—upon the tools at their disposal to do harm. Our thinking, planning and action must be against those capabilities.

Our infrastructure awareness began in 1995, when President Clinton, in PDD-39, tasked the Attorney General to chair a cabinet committee to address the vulnerability of the nation's critical infrastructures. A small working group was formed, the Critical Infrastructure Working Group, which, after working intensely for a period of weeks, recognized that the problem merited working intensely for a period of years, and recommended the creation of a Presidential Commission.

[Slide 3: Critical Infrastructures]

Significant Event One. In July of 1996, President Clinton signed Executive Order 13010, which was in itself an extraordinary step in the brief history of infrastructure assurance. The Executive Order identified eight critical infrastructures so vital that "their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States." They included telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (medical, police, fire, rescue), and continuity of government operations.

The Executive Order created the President's Commission on Critical Infrastructure Protection (PCCIP), and charged the Commission with examining threats to and vulnerabilities of the critical infrastructures; "physical" as well as "cyber." The Commission was also asked to identify legal issues inherent in efforts to protect the infrastructures, and, finally, to recommend a national strategy for their protection.

[Slide 4: PCCIP Commissioners]

It represents a noteworthy vote of confidence in the wisdom of the private sector that the Executive Order didn't just call for an interagency group as a way of reconciling a wide range of potentially conflicting *government* equities. It called for a Commission with equal representation from the public and private sectors to address an issue as pressing to our economic security as our national security.

That is, even before the Commission had studied the problem, and before the Commission had offered its recommendations, the White House had already recognized the unique public-private nature of the problem, and set up a mechanism to arrive at solutions that could get buy-in from both public and private sectors.

Roughly half of the Commissioners were executives from the involved departments and agencies in Washington; the other half were executives from infrastructure companies and organizations bringing industry experience, expertise, and perspective to the Commission. Our Chairman, General Robert "Tom" Marsh, steered us along a public-private path, drawing upon his experience as a former four-star Air Force General and former CEO of Thiokol Corporation.

[Slide 5: PCCIP Final Report]

Significant Event Two. The Commission issued its Final Report, *Critical Foundations*, in October 1997. The final report contains over 70 discrete recommendations—I promise not to review them all here. (In fact, the Commission's Executive Director, Phil Lacombe and I once tried to get through all of the recommendations for a roomful of lawyers. After about 3 hours, we started to run out of gas. (I would bet that the folks in attendance wished we had run out of gas long before that!).

[Slide 6: PCCIP Findings]

In some respects, the Commission's most important finding was that adapting to this challenge requires thinking differently about infrastructure protection. Generally speaking, the Commission found that :

- Vulnerabilities are serious and increasing.
- Information sharing is the most immediate need.
- Responsibility is shared among owners and operators and government.
- The existing legal framework is imperfectly tuned to deal with cyber threats.
- Research and development efforts are inadequate to support infrastructure protection.

[Slide 7: PCCIP Guiding Principles]

Several principles guided the Commission to its recommendations. The Commission recognized that although 90-95% of the critical infrastructures belonged to entities other than the federal government, it would nonetheless be up to government, particularly the federal government, to first demonstrate the seriousness of its commitment to the problem. Once the federal government began to take steps to protect its own critical systems, the Commission believed, the private sector would follow in kind and as most appropriate to protecting their business interests.

The Commission concluded that it would be inappropriate to start thinking in terms of huge government bureaucracies. Instead, the nation should begin by building on existing relationships and relying on existing organizations--as well as relying voluntary cooperation instead of top-down regulatory mandates.

[Slide 8: PCCIP Recommendations]

The Commission's recommendations fell into several categories, including this idea of government leading by example; laying the foundation for a trusted environment necessary for improved information sharing; promoting nationwide awareness about infrastructure protection; conducting necessary research and development; and building structures that embody the public-private partnership. You can read about all of these recommendations in the Commission's report, which remains available, in its entirety, at **Error! Bookmark not defined.**. Many thousands of copies have been downloaded to date.

[Slide 9: Infra assurance functions]

One of the Commission's greatest contributions, in retrospect, came in spelling out exactly what is meant by "infrastructure assurance" or "infrastructure protection." During deliberations, the Commissioners were using those phrases quite a bit. For outsiders, it must have sounded odd to hear talk about whether some measure "promoted infrastructure protection" or "accomplished infrastructure assurance objectives." After thinking about the issues for over a year, the Commission fell into a habit of using those phrases as a shorthand for "everything that should be done to make things better." It meant a great deal to us as Commissioners, but probably meant little to those who did not speak our quaint little private language.

So in preparation for the final report, we made a concerted effort to spell out exactly what was meant by "infrastructure assurance." We arrived at an operational definition that involved five essential elements:

- Policy formulation
- Prevention and mitigation
- Information sharing
- Incident management
- Consequence management

To "do" infrastructure means to do these five things, these five functions, and to constantly improve our ability to do these functions over time. Some of them could be done publicly--predominantly by government; some privately--by industry and individuals. And some could be done only by working in partnership. Information sharing and policy formulation are the best examples of these. After all, imagine a system of information sharing where government only talks to government and companies keep their information close to the vest. Then no one has a complete threat picture—neither government nor the private sector. The process quickly breaks down unless there is honest communication between the public and private sectors.

[Slide 10: Functional Assignments]

The Commission also took a first cut at figuring out *who* would be most suited to doing all of this stuff. Struggling to set aside our industry and agency biases, the Commissioners arrayed all of the various functions and sub-functions on a matrix representing, quite literally, the way the world is arranged. Across the top of the matrix were public versus private responsibilities. Down the side of the matrix were centralized versus decentralized structures. We plotted the functions not according to how some were being performed *today*, but how best they might be accomplished *tomorrow.*

Our conclusions were surprising. It was relatively easy to identify some things that were clearly governmental responsibilities and that needed to be performed in a centralized way—subfunctions represented in the upper left-hand corner of the matrix. Other responsibilities were more effective if done privately and in a decentralized manner--as individual and corporate responsibilities--represented in the lower right-hand corner.

Most extraordinary were the number of responsibilities that fell right in the middle, right in the crosshairs, and how important those things were. Functions as vital to infrastructure assurance as information sharing. Who would do them? Well, that was unclear, because there were literally no structures, no organizations--public or private—located where they needed to be to accomplish them. And so the Commission proposed that some be created.

[Slide 11: PCCIP Proposed Structure]

The Commission proposed—among other things—the creation of a joint public-private information sharing capability, an Information Sharing and Analysis Center (ISAC); and a joint public-private policy formulation capability, a National Infrastructure Assurance Council. Structures that would stand right between the public and private sectors, between federal, state and local governments—structures representing a new level of commitment to partnership specifically in those two areas—policy formulation and information sharing--where partnership is essential to success.

[Slide 12: PDD-63

Significant Event Three. On May 22, 1998, President Clinton announced his new policy on infrastructure protection, titled Presidential Decision Directive 63, or PDD-63 for short.

[Slide 13: PDD Strategic Objectives]

There are six predominant strategic objectives fulfilled by the new policy. I'll spend just a little bit of time on each:

Objective 1: Foundations for partnership. Begin to build trust between government and infrastructure owners and operators starting with sharing of information and joint policy formulation. Ideally, this would include the development of information sharing, analysis, and threat warning capabilities regarding threats to and vulnerabilities of critical infrastructures. It will require the review of existing legal impediments to information sharing, including liability issues and proprietary information protection. As important is ensuring private sector input into policy formulation through a number of channels, including the National Infrastructure Assurance Council and the national planning process.

Objective 2: Elevate National Awareness. Elevate national awareness of infrastructure threat, vulnerability, and interdependency issues through education and other appropriate programs. This may entail for example, a series of conferences to bring together national leaders and highlight the importance of information security. It should involve an examination of the sufficiency of graduate programs in security and K through 12 programs in computer ethics.

Objective 3: Improve assurance management within the federal government. This should be accomplished through the assignment of information assurance responsibilities to Federal agencies' Chief Information Officers, by requiring agencies to develop plans for assuring own critical infrastructures, and by encouraging agencies to participate in simulations and perform vulnerability assessments on key government systems.

Objective 4: Enhance federal protection and assurance efforts. The intent is to identify and encourage legislation that would increase the effectiveness of federal infrastructure assurance and protection efforts. This will require reviewing the sufficiency of current laws through interagency process, studying impediments to public-private information sharing, reviewing the procurement process, and incorporating assurance objectives into the planning framework of the Government Performance and Results Act (GPRA).

Objective 5: Increase R&D investment. Improve infrastructure assurance research and development through better focus and coordination. This can be done by articulating research priorities such as the development of enhanced intrusion detection and network monitoring tools and enhanced coordination of research and development efforts among departments and agencies by the Office of Science and Technology Policy.

Objective 6: Build structures to embody the partnership. Establish national structures to facilitate effective partnerships among public, private and municipal sectors.

[Slide 14: PDD Organization

A little bit more on the organizations created by PDD-63. One observation that received powerful validation from the Commission's Advisory Committee was that where infrastructures are concerned, what might be good for one might not be good for all. That is, the courses of action that might be best for the telecommunications industry might not be best for electric power or for transportation. Some measures may need to be implemented infrastructure by infrastructure, or at least at different rates or in different ways across the infrastructures. This principle is reflected in the organizational scheme of the Administration's policy.

[Slide 15: PDD Structure]

One major goal is to arrive at a joint public-private, infrastructure-by-infrastructure planning process, one that is highly "sector" driven. Federal lead agencies, such as the Department of Transportation for the transportation industry, Treasury for banking and finance, etc., each identify a *Sector Liaison Official* who, along with a designated *Sector Coordinator* from the industry, meet and prepare input into the *National Infrastructure Assurance Plan*. The Plan, or NIAP, is a multi-year effort aimed at encouraging the infrastructure sectors to assess and reduce their vulnerabilities, and identify, prevent, contain and rebuff attacks on their critical infrastructures.

In addition, the Sector Liaison Officials meet regularly under the auspices of the National Security Council as the *Critical Infrastructure Coordinating Group* (CICG), an interagency process that provides a forum for representatives to compare similarities and articulate differences between the infrastructures they represent.

Despite differences, however, the policy also recognizes the need for a single focal point within the Administration to coordinate agency efforts, and particularly to encourage attention to infrastructure interdependencies. So the President named Richard Clarke as his National Coordinator for Security, Infrastructure Protection and Counter-terrorism, to report to him through the National Security Advisor. An important responsibility of *the Critical Infrastructure Assurance Office* (CIAO) is to help the National Coordinator and the CICG assemble the NIAP, and assist in the coordination of education, awareness, legislative and public affairs efforts.

The policy also identifies structures to begin to meet government and industry's demand for more and better threat and vulnerability information. This is to be accomplished through dual structures, one housed at the FBI, and another (or others) in the private sector—Information Sharing and Analysis Centers (ISACs)--for information that might not otherwise flow through traditional law enforcement channels.

[Slide 16: Org chart (draft)]

Well, that's a "quick" overview of the functions identified by the PCCIP, and the first steps taken by the Administration in response. And if it looks and sounds complex, well, that's because it is! Which is yet another finding we can attribute to the Commission:

If there is one thing we learned hashing out these issues over a year-and-a-half it is that the grand solutions we each carried to the table and favored at the outset turn out not to provide entirely complete or satisfactory solutions. There is no magic *single* solution--no "one thing" that either government or the private sector can do to assure the infrastructures.

When we really studied the problem, we recognized that it was just too big, too pervasive, too ambitious, too expansive, too *expensive*, for either the private sector or the government alone to handle. It requires cultural change across the board--*fundamental* changes, over time, in the way businesses manage risk, governments align themselves, and people act at home and work.

Likewise, it should go without saying that there is no single agency or office that can do it alone—although many agencies have already made great strides:

The superior planning and preparedness capabilities of the Department of Defense are unparalleled anywhere and will contribute greatly to our national planning effort. DoD has, in fact, recently undertaken a series of of initiatives and organizational changes to better protect its own critical resources and to contribute appropriately to a national response capability. But because the first indications of an attack on the U.S. are likely to come from correlation of seemingly unrelated domestic incidents, development of a meaningful system of indication and warning must be undertaken in close cooperation with law enforcement domestically, and the intelligence community operating abroad.

Likewise, the Department of Justice and the FBI have learned a great deal about investigating incidents in electronic environments. And the FBI has made great strides in building up an investigative capability—First with the CITAC, which combined criminal, counterintelligence and counter-terrorism techniques and information, and now with the National Infrastructure Protection Center.

Effective criminal response is our most powerful deterrent. But it is not all of infrastructure protection. After all, the fact that making and setting off a truck bomb is a crime did not prevent the World Trade Center and Oklahoma City tragedies, it did not mitigate the effects of those blasts, nor did it help victims recover. It is not the whole solution.

There are also substantial and continuing roles in infrastructure assurance for agencies and offices such as the National Economic Council, the Department of Commerce, state and local governments, owners and operators of the critical infrastructures (of course), and the international community.

It should be similarly apparent that the measures I have spoken of today, PDD-63, the Administration's "first steps," are not all of what will eventually be required. After all, a PDD states policy, but is not a funding vehicle. It cannot allocate funds where they might be needed. It cannot, on its own, build structures outside of government, structures like the ISAC. It cannot change laws of Congress. It cannot, in itself, promote international cooperation. But it is a step in the right direction to accomplish all of these things, and now it is up to us to make this policy a part of the way we go about our business—public and private.

Thank you for the kind invitation to be with you today. I hope you will be able to make the most of the terrific program that the NDIA has assembled.

PCCIP to PDD:
First Steps in
Infrastructure Assurance

**National Defense Industrial Association
14th Annual Security Technology
Symposium and Exhibition
June 15-18, 1998**

stevan.mitchell@pccip.gov

Recent Events in “Infrastructure Assurance”

E. O. 13010

- Commission
- Advisory Committee
- Interagency review

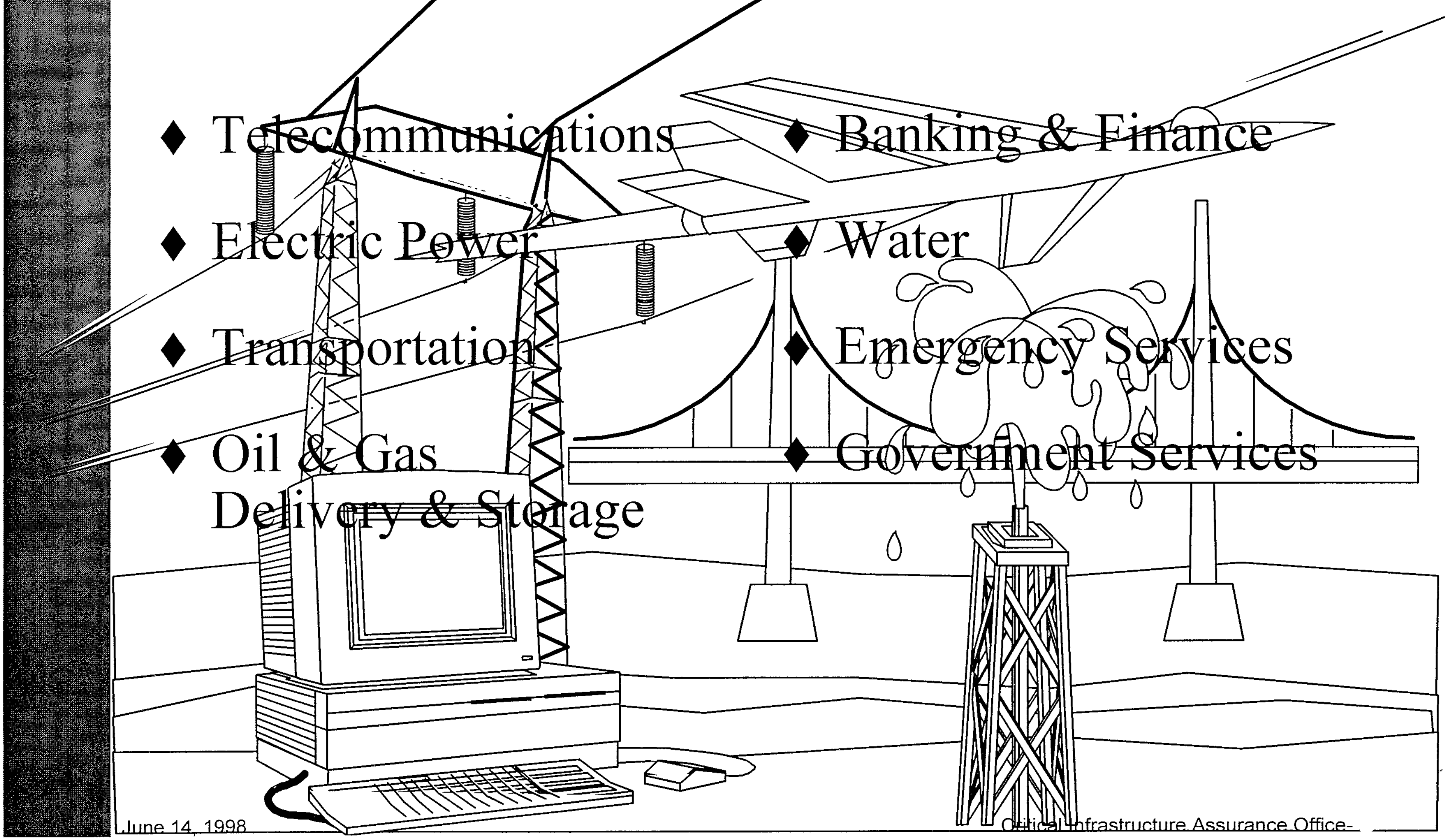
PCCIP Final Report

- Federal government lead
- Information flow
- Partnership

PDD 63

- Executive branch “first steps”
- Structures for partnership

Executive Order 13010: Critical Infrastructures



- ♦ Telecommunications
- ♦ Electric Power
- ♦ Transportation
- ♦ Oil & Gas Delivery & Storage
- ♦ Banking & Finance
- ♦ Water
- ♦ Emergency Services
- ♦ Government Services

June 14, 1998

Critical Infrastructure Assurance Office-

PCCIP Commissioners

Public Sector

CIA

FBI

FEMA

NSA

Department of Commerce

Department of Defense

Department of Energy

Department of Justice

Department of Transportation

Department of Treasury

Private Sector

AT&T

IBM

Federal Reserve Board

Georgetown University

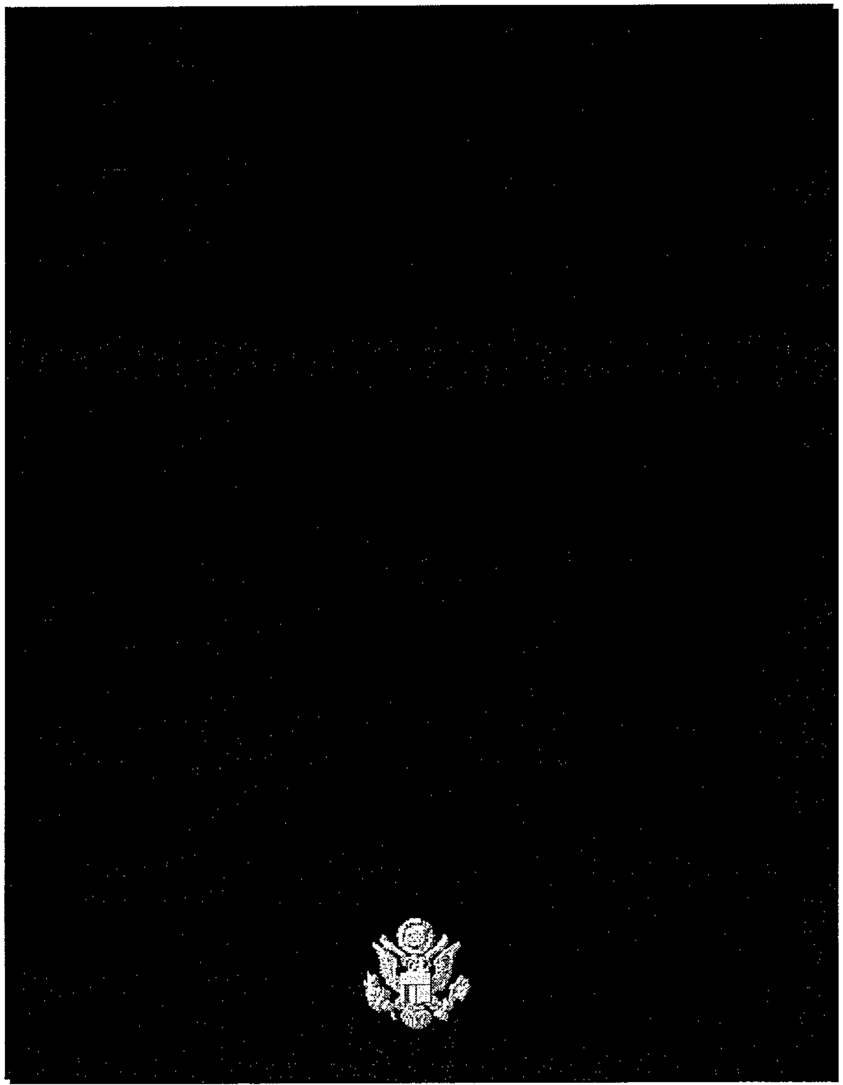
National Association of Public Utility Regulators

Pacific Gas & Electric

Thiokol Corporation

Association of American Railroads

October 1997: PCCIP Report



PCCIP Findings

- ♦ The challenge is adapting to a changing culture
- ♦ Vulnerabilities are serious and increasing
- ♦ Information sharing is the most immediate need
- ♦ National warning & analytic capabilities are lacking
- ♦ Government and industry are not prepared
- ♦ Legal framework needs modernization
- ♦ R&D and investment are not sufficient

PCCIP Guiding Principles

- Government must lead by example
- Start with owners and operators
- Build on that which exists
- Promote voluntary cooperation
- Maintain existing oversight and regulation
- Practice continuous improvement

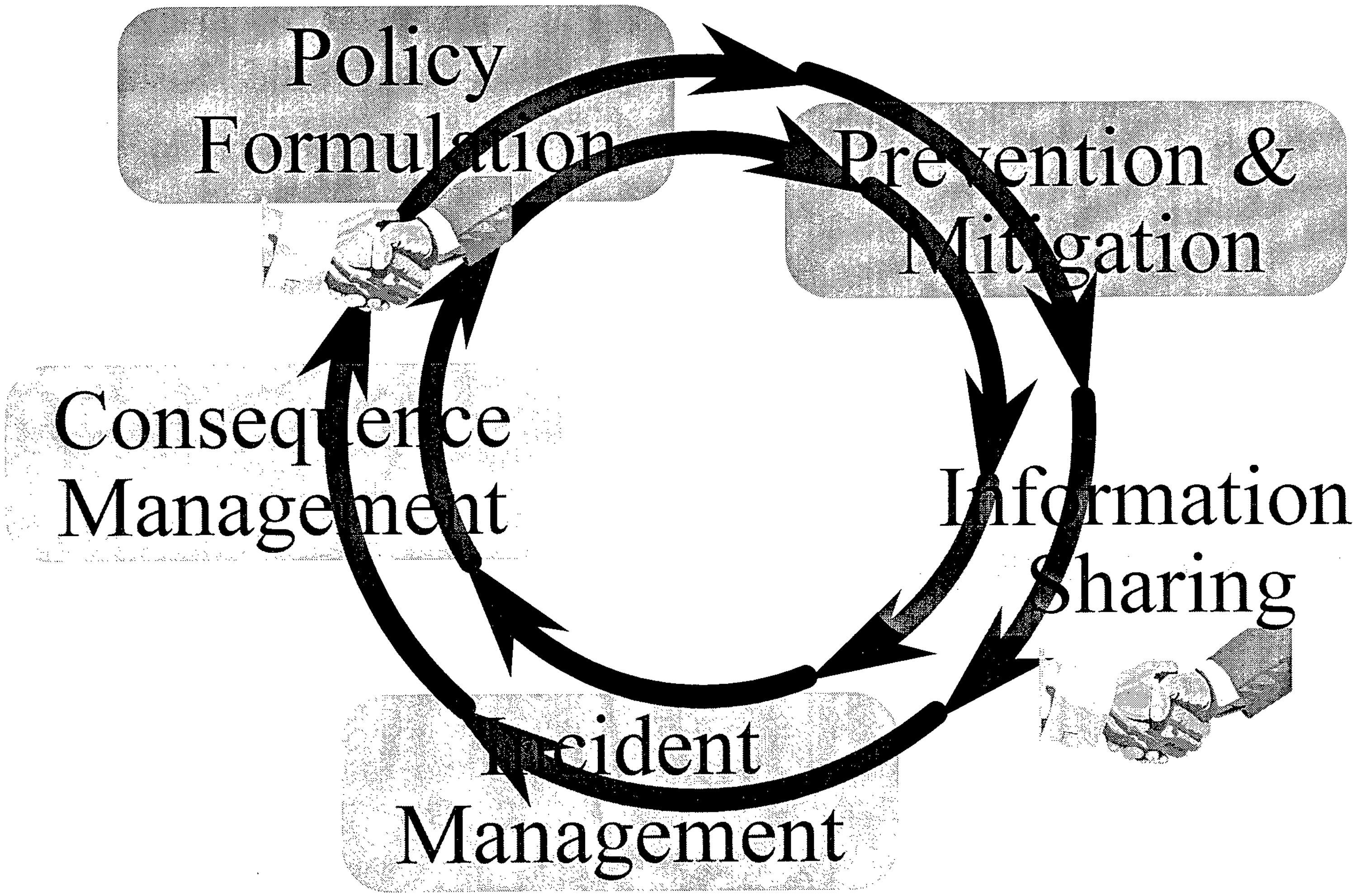
PCCIP Recommendations

GOALS

- ✪ *Improve coordination*
- ✪ *Establish infrastructure assurance roles*
- ✪ *Foster partnerships*
- ✪ *Coordinate global interests*

- ♦ Information Sharing
- ♦ Leading by Example
- ♦ Education & Awareness
- ♦ Research & Development
- ♦ Federal Assistance
- ♦ Legal Initiatives
- ♦ Structuring the Partnership

Infrastructure Assurance Functions



Policy Formulation

Prevention & Mitigation

Information Sharing

Incident Management

Consequence Management

June 14, 1998

Critical Infrastructure Assurance Office-

"Location" of Infrastructure Assurance Functions

Centralized

Decentralized

Public Roles

Federal Roles

- **Plan for Integrated Law Enforcement, Intelligence & Military Response**
- **Estimate the Emerging Threat & Changing Vulnerabilities**
- **Manage Response & Recovery**
- **Analyze Information & Prepare Threat Advisories**
- **Issue the National Policy**
- **Assess National Risk**
- **Disseminate Warnings**
- **Coordinate Research & Development**

Propose national strategy & objectives

- Plan law enforcement & military actions
- Manage response & execution of law enforcement & military actions
- Influence private sector investment

State & Local Roles

- Plan response & recovery (people/property)
- Manage response & recovery (people/property)
- Defensive protection initiatives
- Assess & promote new regulations

Private Roles

Trade & Industry Associations

- Set assurance standards, certification, best practices
- Research & Development
- Defensive protection initiatives

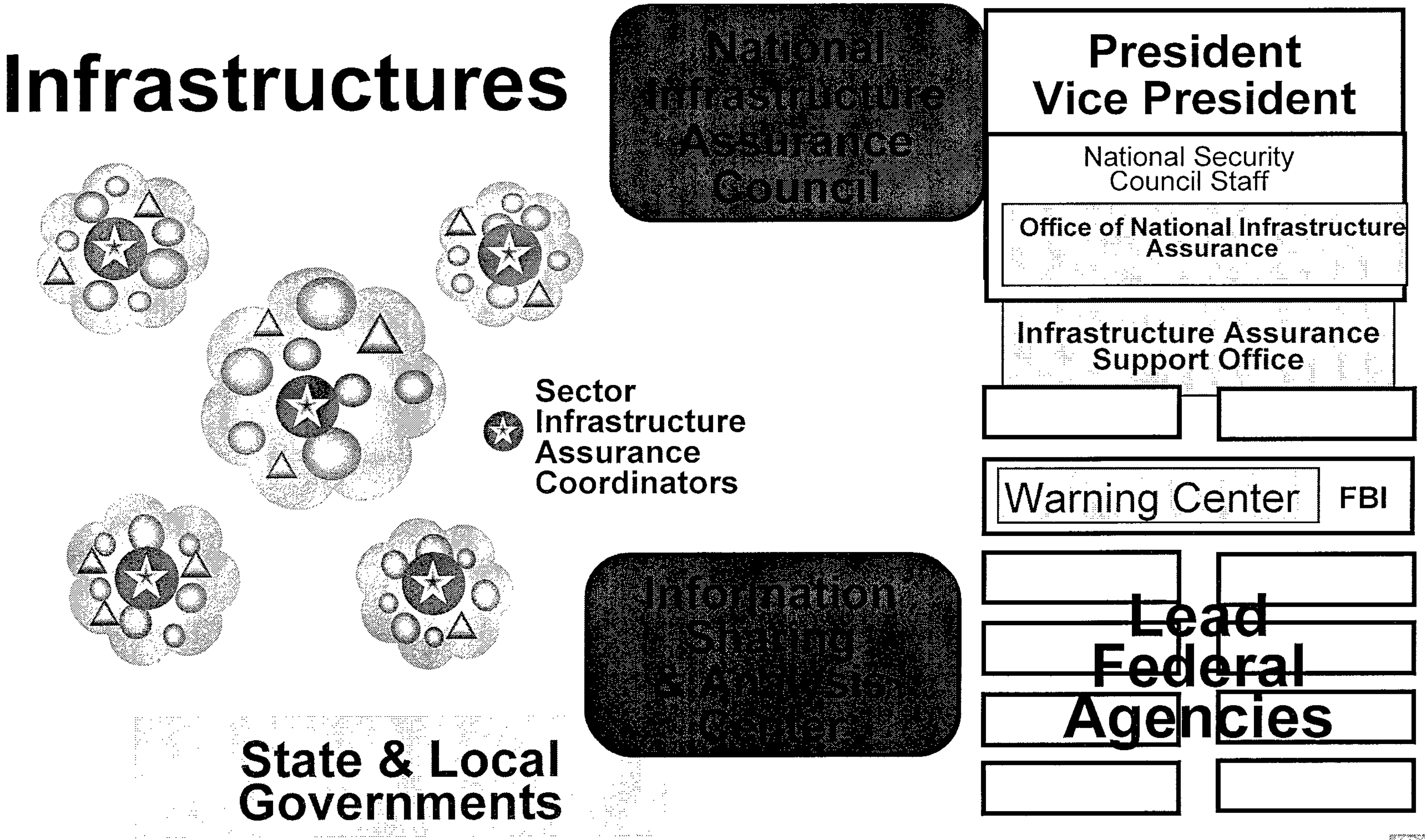
- **Share information**
- Develop education & awareness
- Negotiate funding
- Manage & enforce implementation
- Propose & promote new regulation
- Control misinformation
- Integrate public/private perspective
- Shape international environment
- Maintain public confidence

- Plan restoration
- Manage restoration

Internal Processes & Market Forces

- Assess Vulnerabilities & Risk of System Components
- Manage Operations Consistent with Best Practices
- Acquire resources for Protecting Systems
- Defensive protection initiatives
- Research & Development

Proposed Structure for Infrastructure Assurance



Infrastructures

National Infrastructure Assurance Council

President
Vice President

National Security Council Staff

Office of National Infrastructure Assurance

Infrastructure Assurance Support Office

Sector Infrastructure Assurance Coordinators

Warning Center

FBI

Information Sharing & Analysis Center

Lead Federal Agencies

State & Local Governments

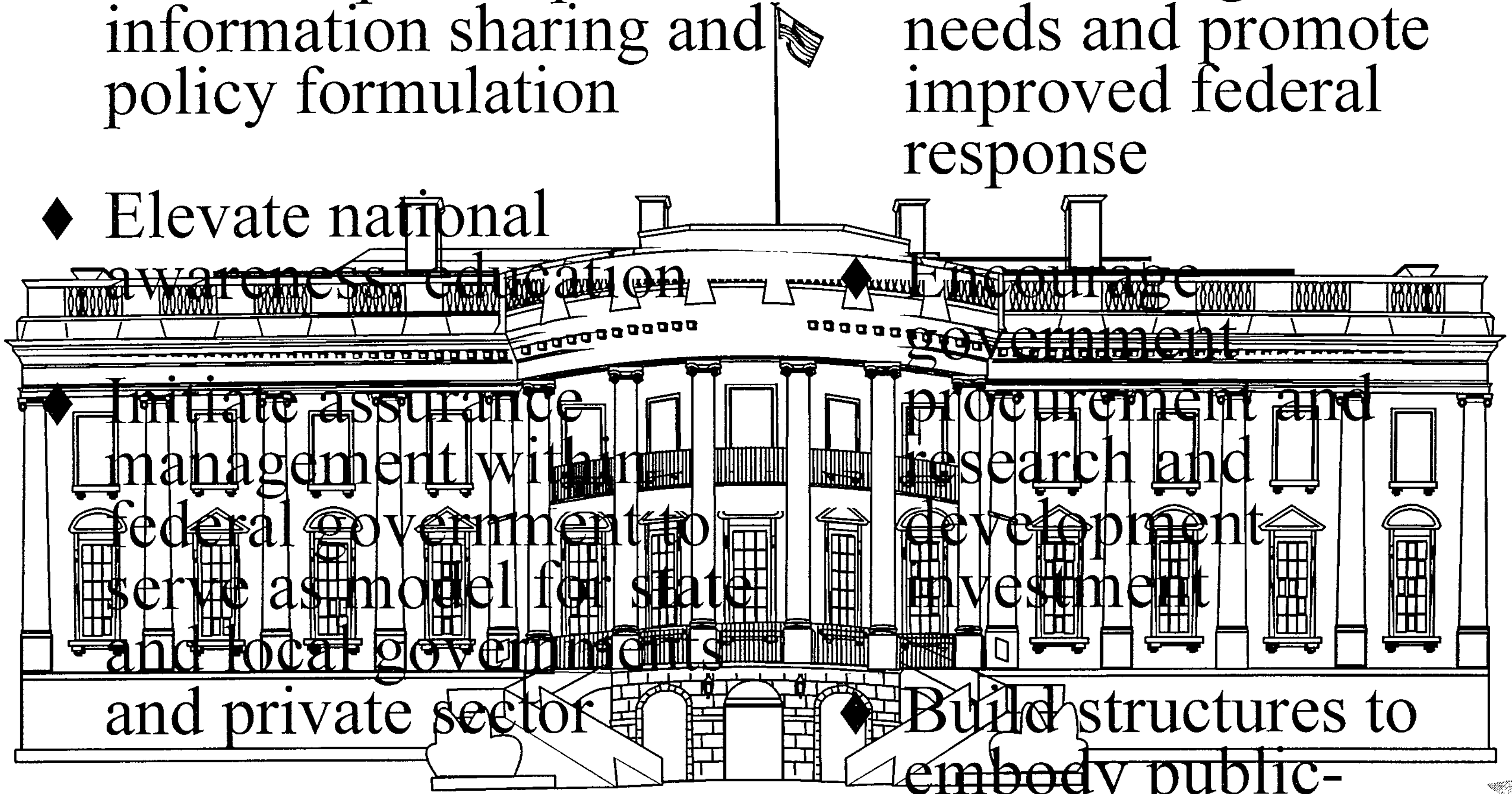
June 14, 1998

Critical Infrastructure Assurance Office-

May 1998: Presidential Decision Directive 63

Critical Infrastructure Protection

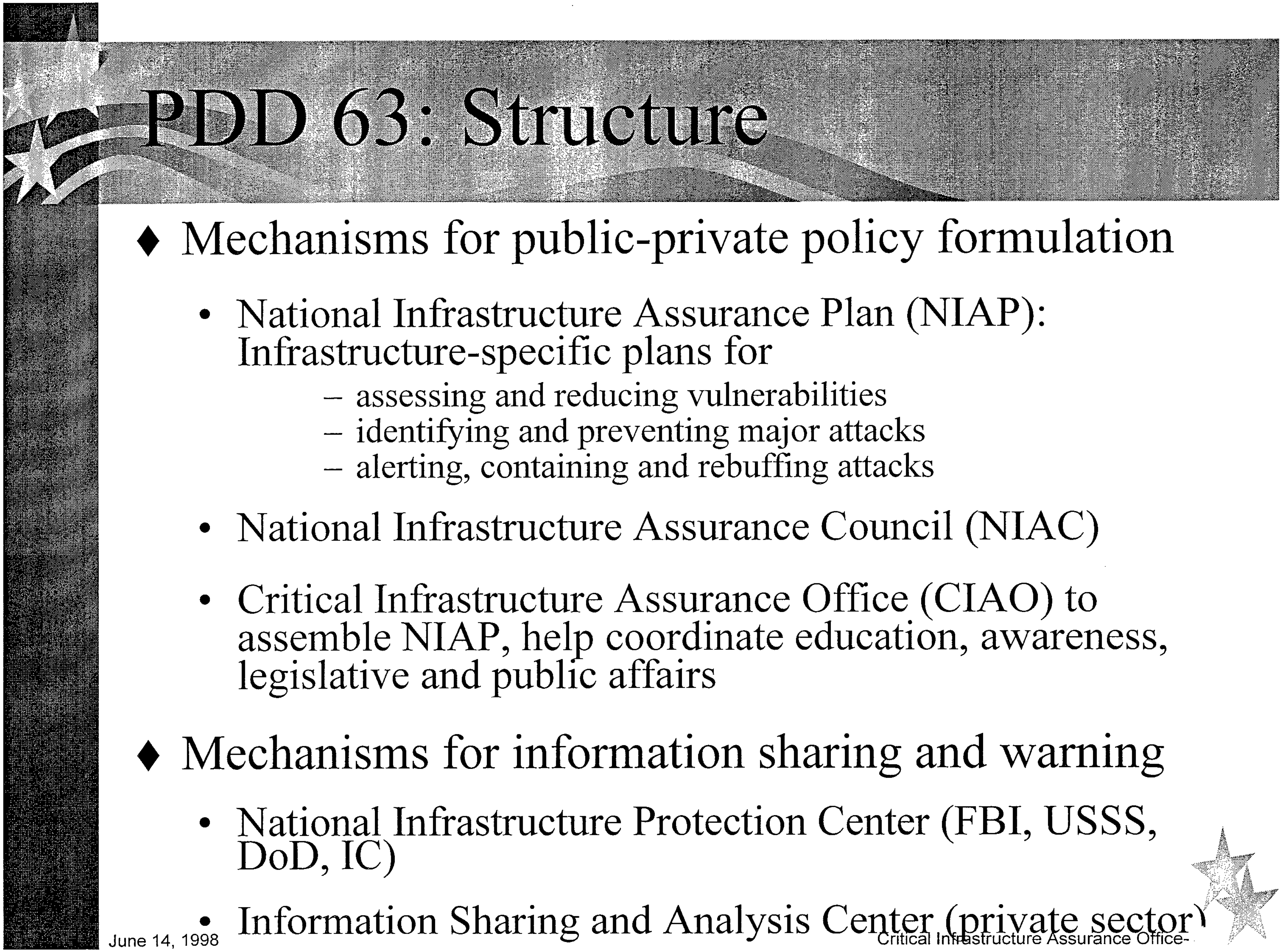
PDD 63: Strategic Objectives



- ♦ Promote public-private information sharing and policy formulation
- ♦ Elevate national awareness, education
- ♦ Initiate assurance management within federal government to serve as model for state and local governments and private sector
- ♦ Evaluate legislative needs and promote improved federal response
- ♦ Encourage government procurement and research and development investment
- ♦ Build structures to embody public-private partnership

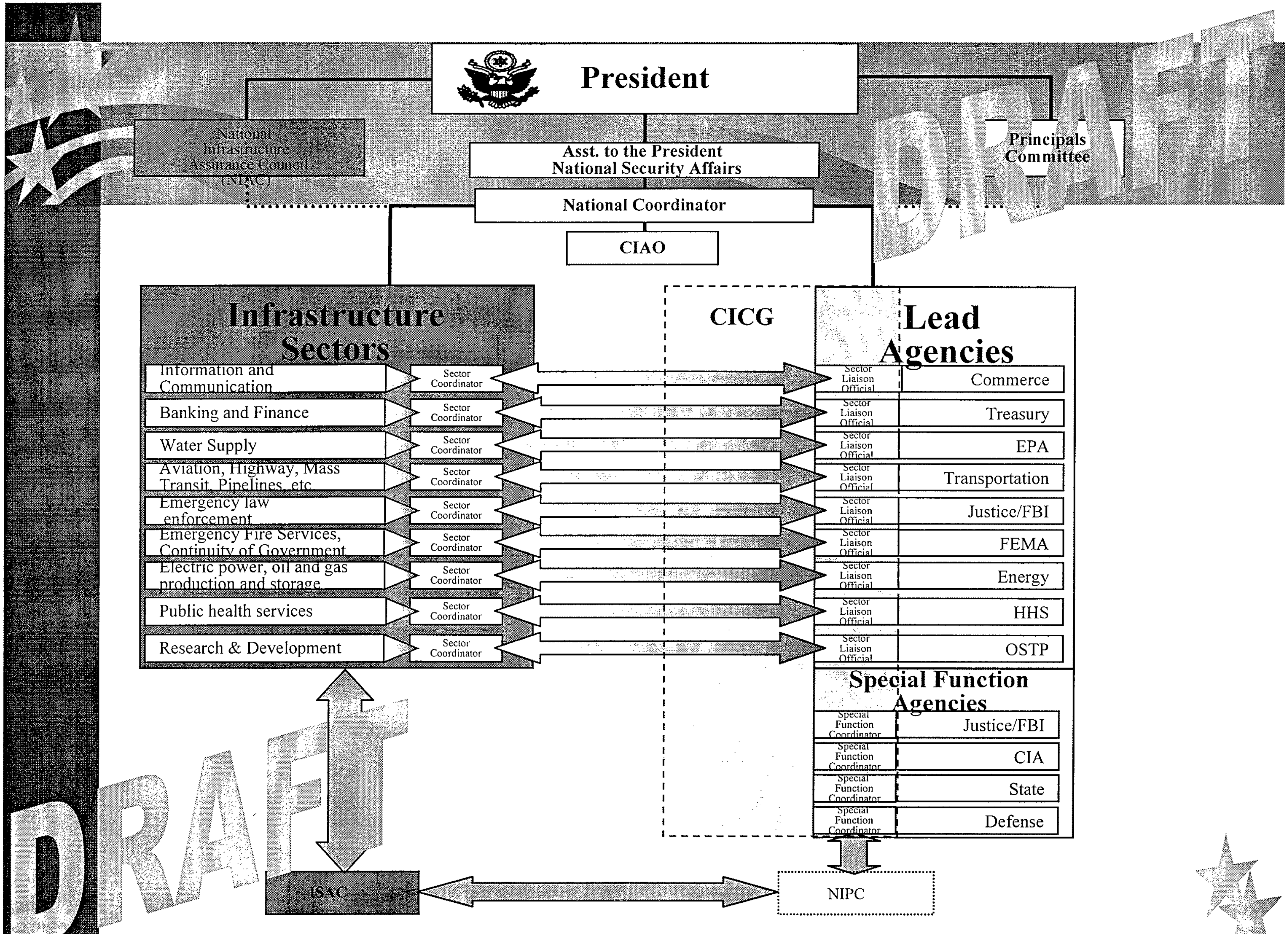
PDD 63: Organization

- ♦ "Sector" driven:
  - Lead Agencies for Sector Liaison (Sector Liaison Officials)
  - Sector Coordinators (private sector)
  - Lead Agencies for Special Functions (Functional Coordinators)
- ♦ Interagency process provides focal point for federal efforts, sector interdependencies
  - National Coordinator for Security, Infrastructure Protection and Counterterrorism (within NSC)
  - Interagency Coordinating Group (CICG)



PDD 63: Structure

- Mechanisms for public-private policy formulation
  - National Infrastructure Assurance Plan (NIAP): Infrastructure-specific plans for
    - assessing and reducing vulnerabilities
    - identifying and preventing major attacks
    - alerting, containing and rebuffing attacks
  - National Infrastructure Assurance Council (NIAC)
  - Critical Infrastructure Assurance Office (CIAO) to assemble NIAP, help coordinate education, awareness, legislative and public affairs
- Mechanisms for information sharing and warning
  - National Infrastructure Protection Center (FBI, USSS, DoD, IC)
  - Information Sharing and Analysis Center (private sector)



President
National Infrastructure Assurance Council (NIAC)
Principals Committee
Asst. to the President National Security Affairs
National Coordinator
CIAO
Infrastructure Sectors
Information and Communication
Banking and Finance
Water Supply
Aviation, Highway, Mass Transit, Pipelines, etc
Emergency law enforcement
Emergency Fire Services, Continuity of Government
Electric power, oil and gas production and storage
Public health services
Research & Development
Sector Coordinator
CICG
Lead Agencies
Sector Liaison Official
Commerce
Treasury
EPA
Transportation
Justice/FBI
FEMA
Energy
HHS
OSTP
Special Function Agencies
Special Function Coordinator
Justice/FBI
CIA
State
Defense
ISAC
NIPC

June 14, 1998

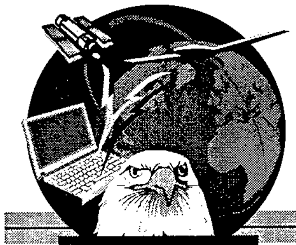
Critical Infrastructure Assurance Office-

New Dimensions in Security Threats and Countermeasures

The International Threat

Major General John P. Casciano

HQ USAF / XOI



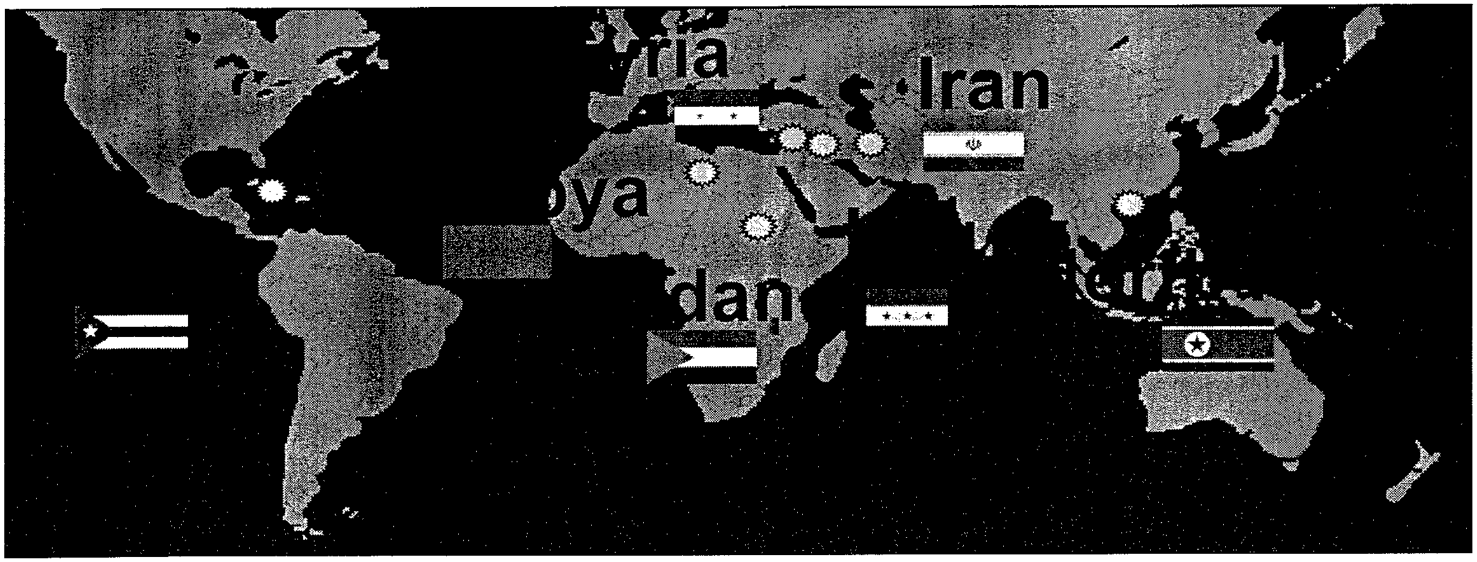
What I'll Talk About

- The Actors
- The Weapons
- Threat Megatrends

The Actors
State Sponsors

- "Pariah" states
- Weapon of state policy

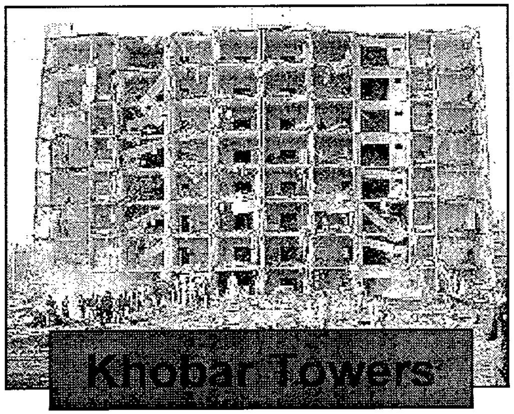
Pan Am 103



The Actors

National/Transnational Groups

- **US State Dept recognizes 30 Foreign Terrorist Organizations**
  - Seeking political goals
  - Fueled by religious extremism
  - Motivated by economic incentives

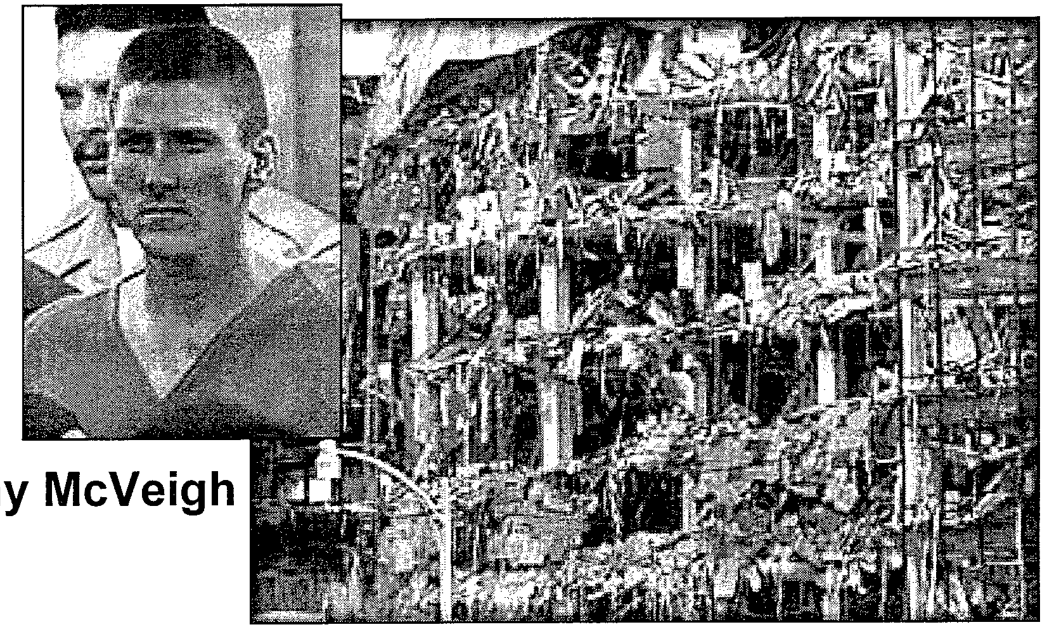


Khobar Towers

Abu Nidal Organization (Libya)	Kurdistan Workers' Party (Turkey)
Abu Sayyaf Group (Philippines)	Liberation Tigers of Tamil Eelam (Sri Lanka)
Armed Islamic Group (Algeria)	Manuel Rodriguez Patriotic Front Dissidents (Chile)
Aum Shinrikyo (Japan)	Mujahedin-e Khalq Organization (Iran)
Euzkadi Ta Askatasuna (Spain/France)	National Liberation Army (Colombia)
Dem. Front for Lib. of Palestine	Palestine Islamic Jihad
Hamas (Israel/Jordan)	Palestine Liberation Front (Iraq)
Harakat ul-Ansar (Pakistan)	Pop. Front for the Lib. of Palestine
Hizballah (Lebanon)	[illegible]
Gama'a al-Islamiyya (Egypt)	[illegible]
Japanese Red Army	[illegible]
al-Jihad	[illegible]
Kach (Israel)	[illegible]
Kahane Chai (Israel)	[illegible]
Khmer Rouge (Cambodia)	Tupac Amaru Revolutionary Movement (Peru)

The Actors
Individuals

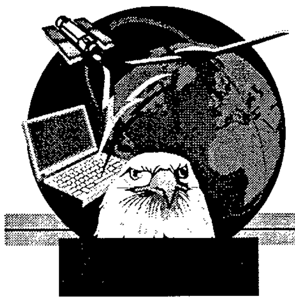
- Wildcard threat
  - Increasingly lethal tools available
  - Nearly impossible to foresee



Timothy McVeigh

April 19, 1995

Usama Bin Ladin

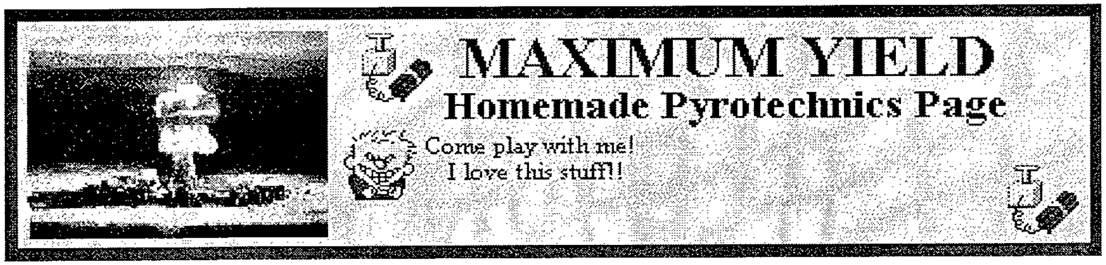


What I'll Talk About

- The Actors
- The Weapons
- Threat Megatrends

The Weapons
Conventional Explosives

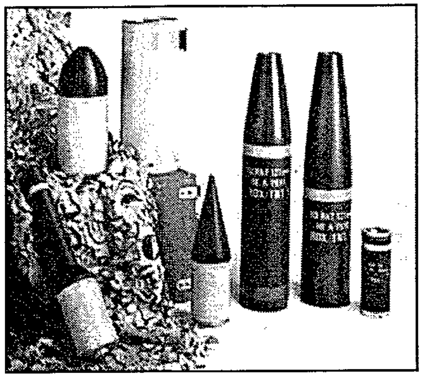
- From bombs to advanced missiles
  - Readily available
  - Effective...and cheap

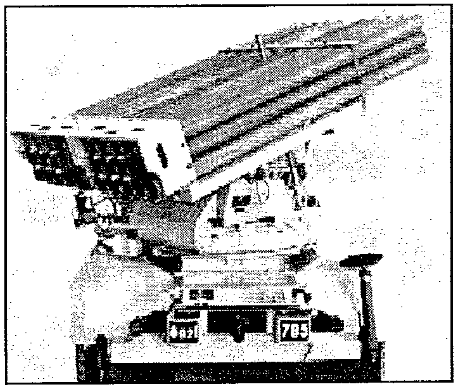

MAXIMUM YIELD

Homemade Pyrotechnics Page

Come play with me!
I love this stuff!!

Open Market Price of SA-7: $50,000





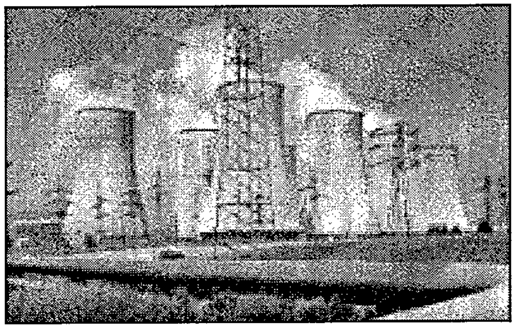
The Weapons
Weapons of Mass Destruction

[redacted]

- Chemical/Biological
  - Increasing non-state interest
  - Knowledge and technology widely available

Aum Shinrikyo Sarin Attack
12 Killed; 5,500 Hospitalized

- Nuclear
  - Little chance of high-yield bomb
  - Radiological threat more likely

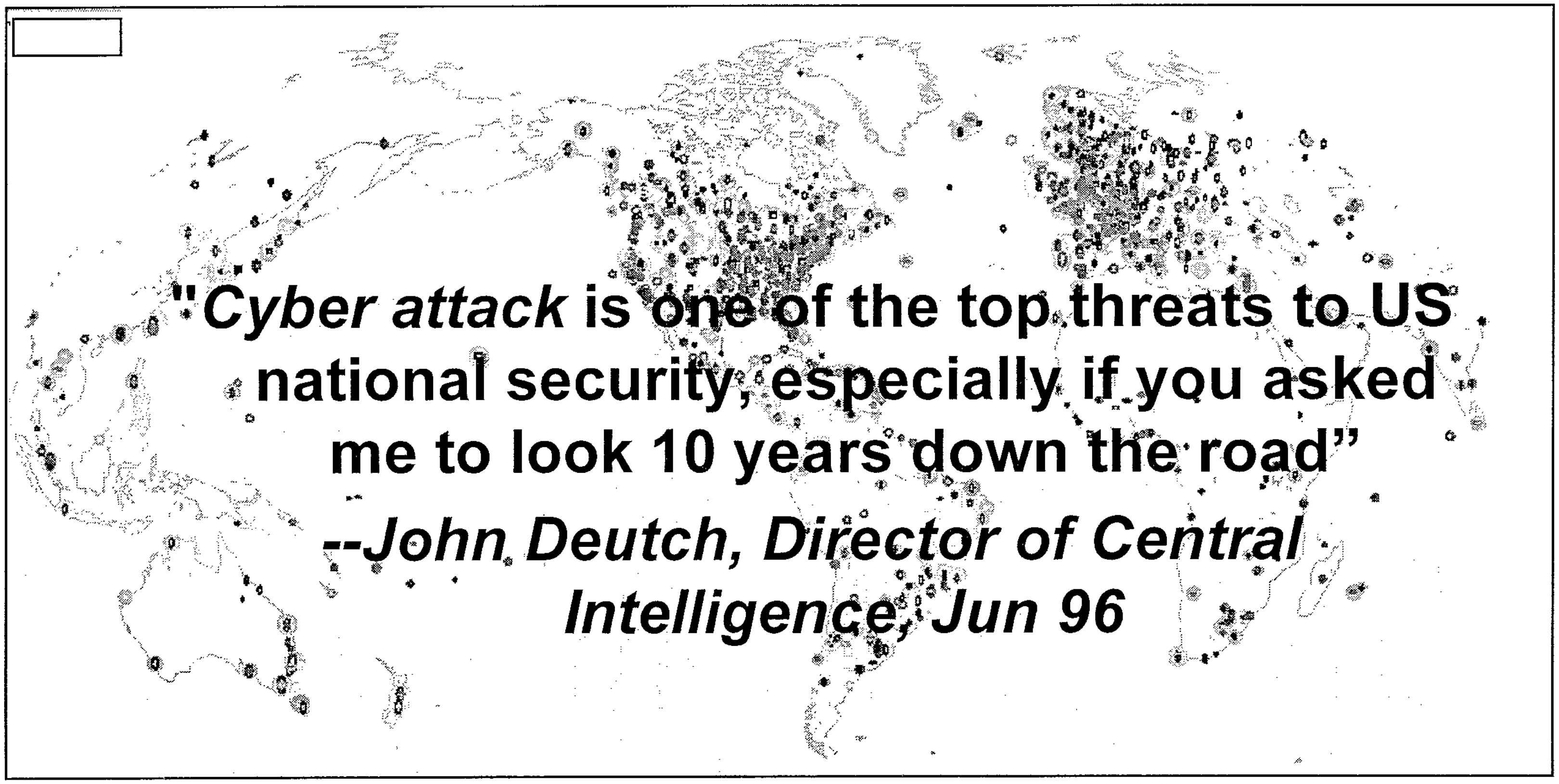


[redacted]

The Weapons

Information Technology

- If you can point and click, you can hack...



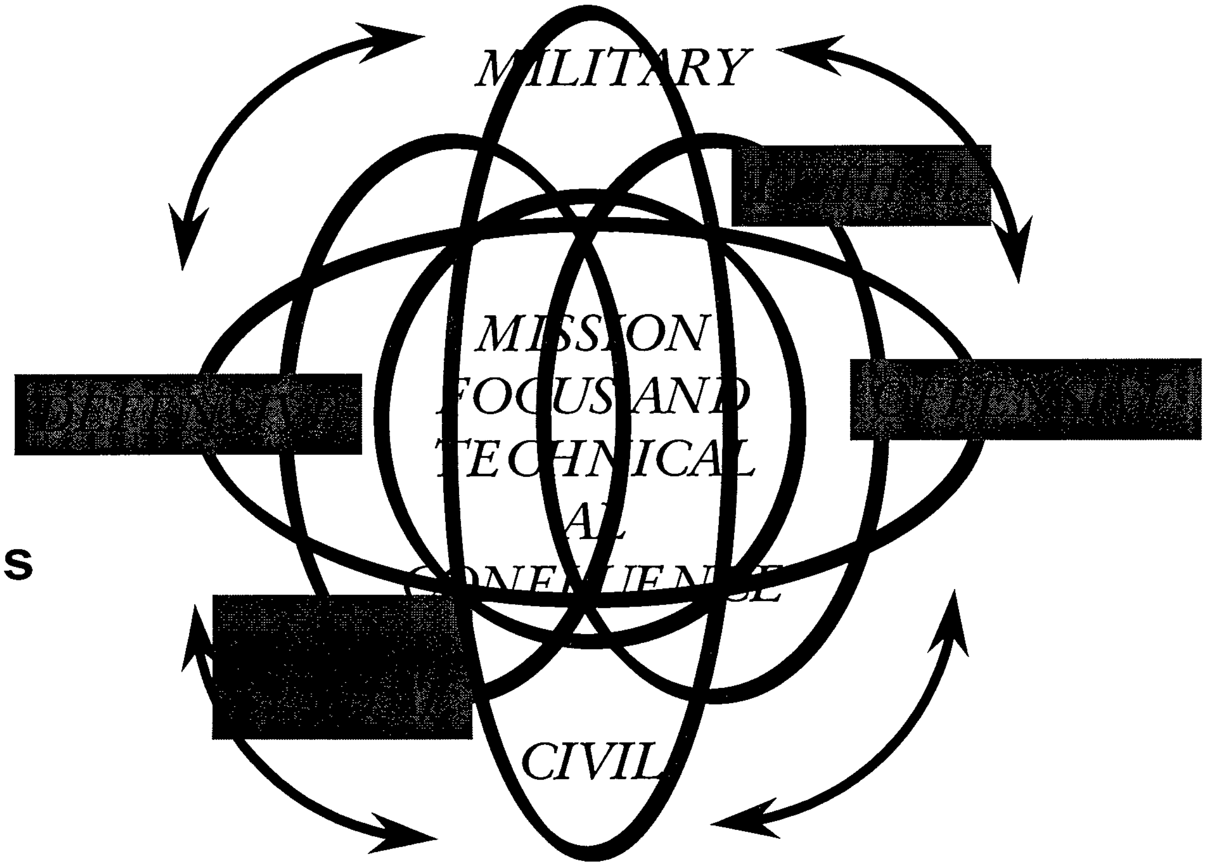
"*Cyber attack* is one of the top threats to US national security, especially if you asked me to look 10 years down the road"

--John Deutch, Director of Central Intelligence, Jun 96

Worldwide Net Hosts - 1997

The Weapons
Information Warfare

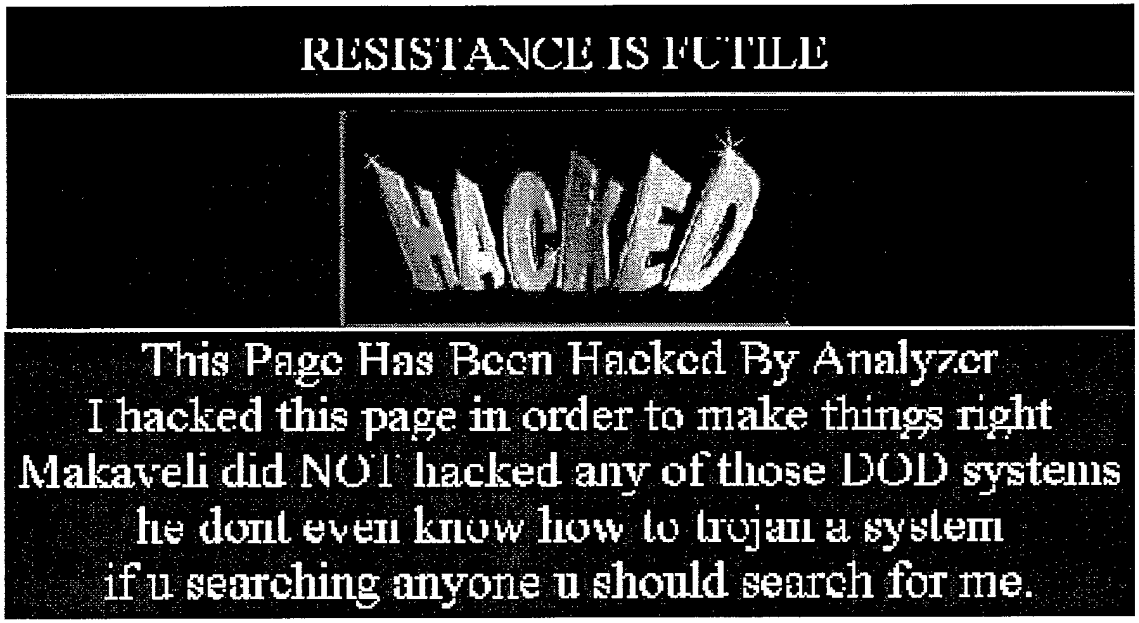
- **Most military organizations...**
  - Rely on computers
  - Use commercial communications
  - Are connected to parent organizations via the INTERNET



The Weapons

Information Warfare

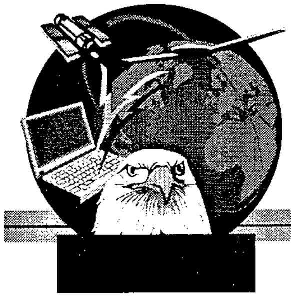
- **Most military organizations...**
  - Rely on computers
  - Use commercial communications
  - Are connected to parent organizations via the INTERNET



RESISTANCE IS FUTILE

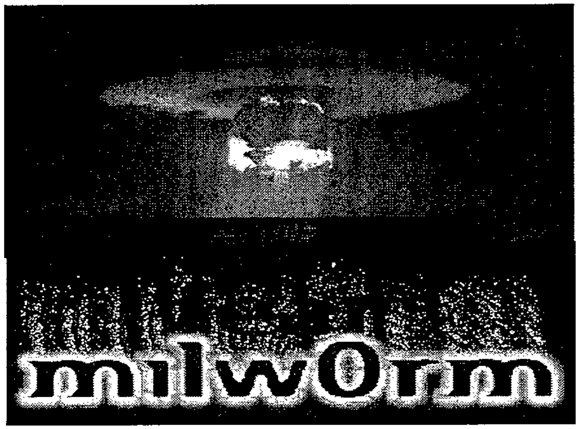
This Page Has Been Hacked By Analyzer
I hacked this page in order to make things right
Makaveli did NOT hacked any of those DOD systems
he dont even know how to trojan a system
if u searching anyone u should search for me.

Hacked INTERNET Page Claiming Responsibility for DoD Intrusions



The Weapons
Information Warfare

- Cyber Attack
  - Infiltration of Indian computer systems containing nuclear data
- Psyops
  - Unlimited potential to manipulate information
  - Homepages to advance message, plan activity



Message Left on Hacked Indian System

INTERNET

Tamil Eelam homepage

AUM Shinrikyo

VOZ REBELDE
ORGANO OFICIAL DEL MOVIMIENTO REVOLUCIONARIO TUPAC AMARU

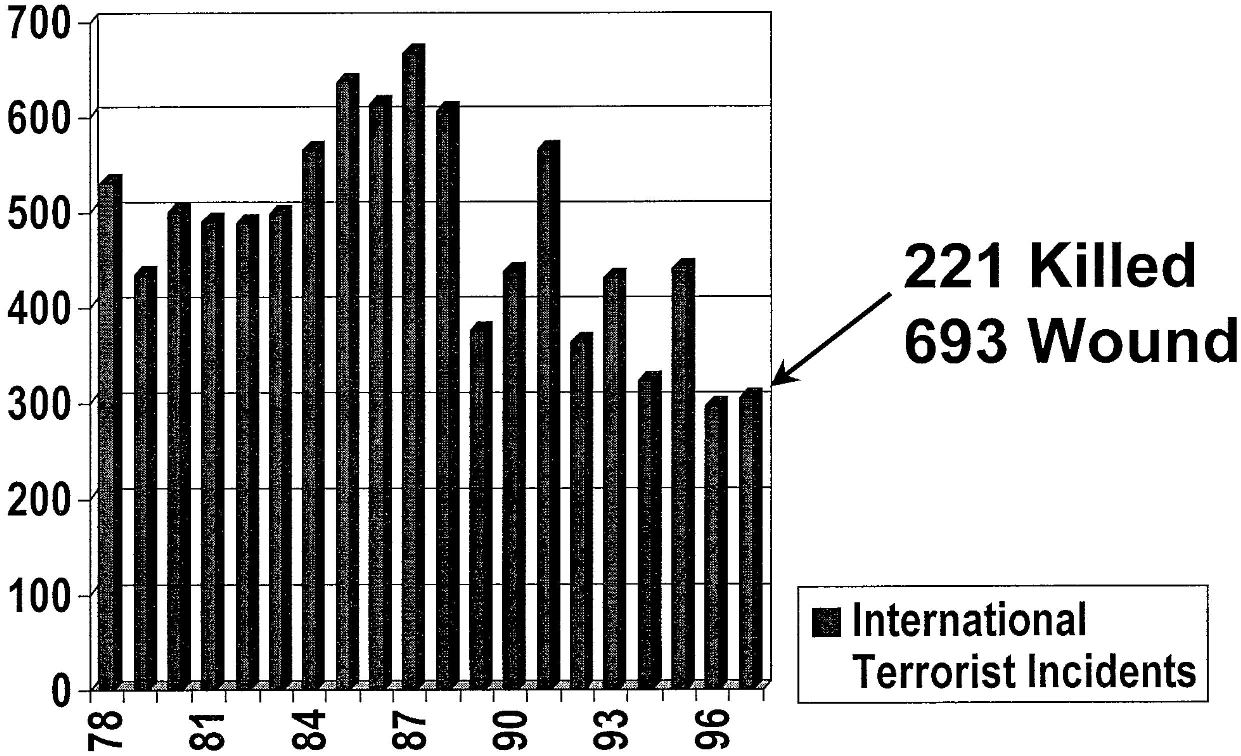
FARC-EP COMISION INTERNACIONAL

What I'll Talk About

- The Actors
- The Weapons
- Threat Megatrends

Threat Megatrends

- Number of terrorist acts has declined ... casualties have increased

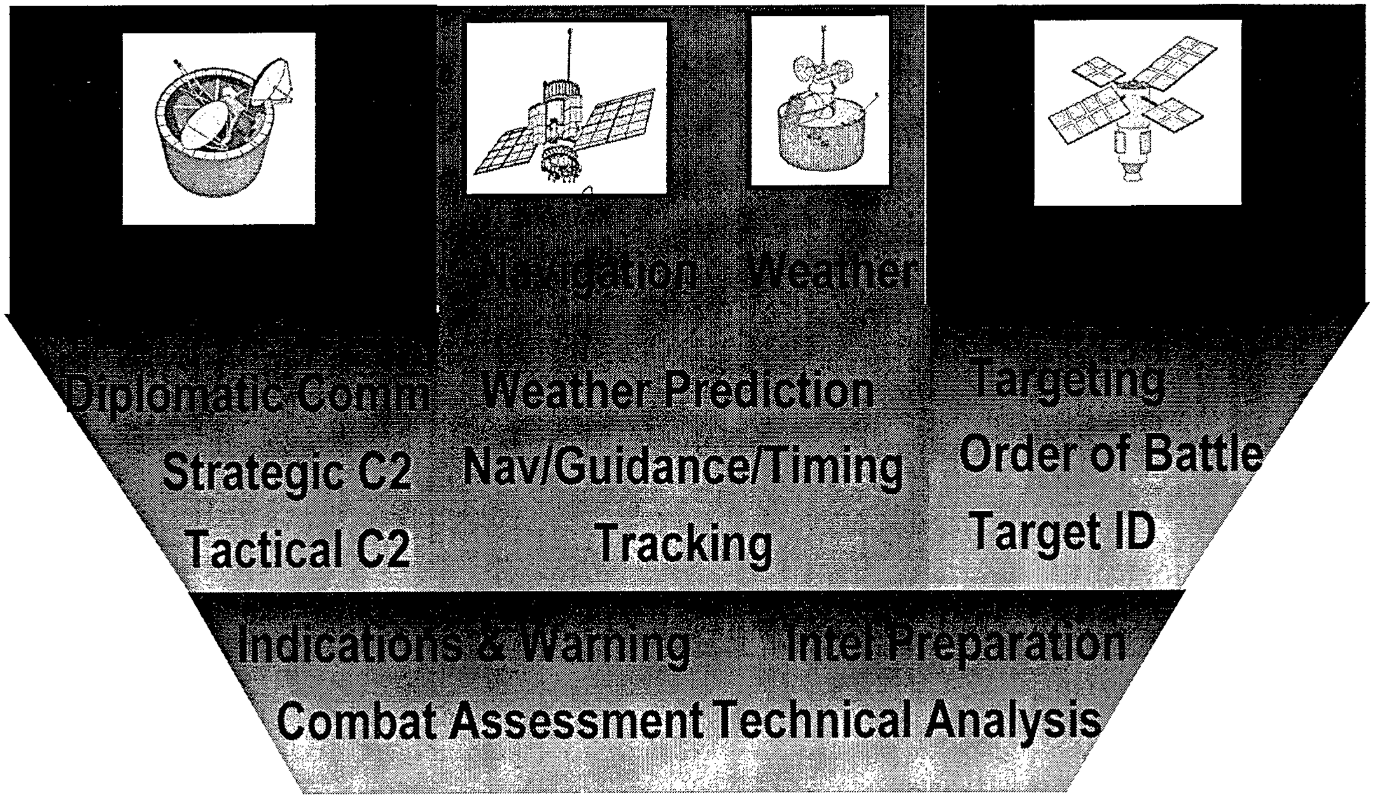


221 Killed
693 Wounded

Threat Megatrends

Tools and Methods Have Changed

- Use of Space and Internet for intelligence, planning, and communications



Navigation Weather

Diplomatic Comm
Strategic C2
Tactical C2

Weather Prediction
Nav/Guidance/Timing
Tracking

Targeting
Order of Battle
Target ID

Indications & Warning Intel Preparation
Combat Assessment Technical Analysis

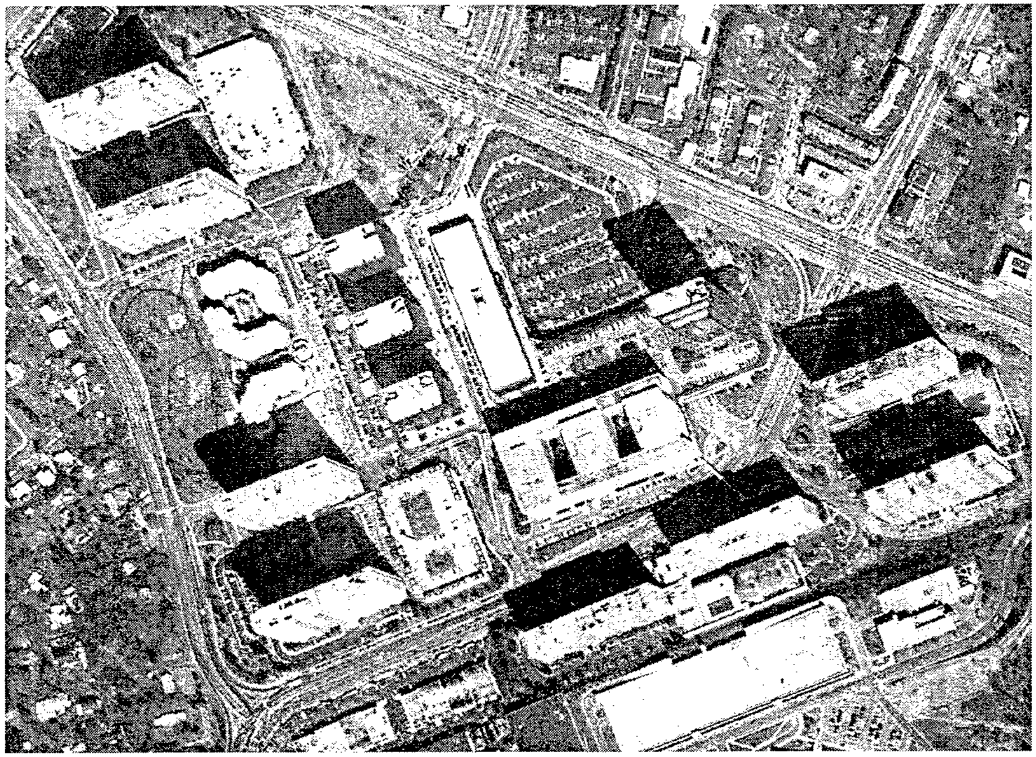
Threat Megatrends

Tools and Methods Have Changed

- Use of Space and Internet for intelligence, planning, and communications

Federation of
American
Scientists

Intelligence
Resource
Program



1-Meter Resolution Imagery Posted on Internet

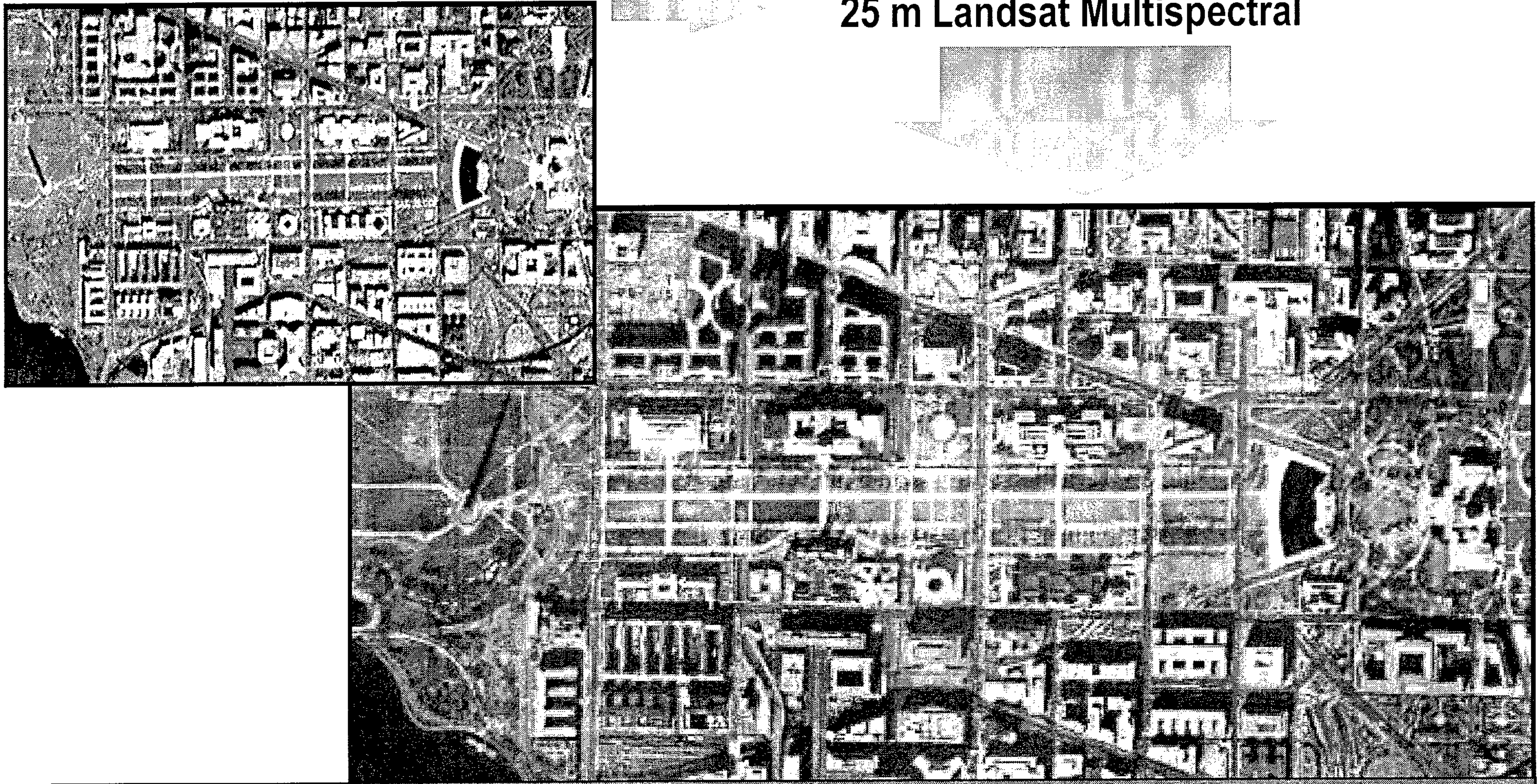
Threat Megatrends

Tools and Methods Have Changed

[redacted]

2 m Russian Panchromatic

Fused with
25 m Landsat Multispectral



Potential Adversaries Have Access to Military-Quality Imagery

Threat Megatrends

Tools and Methods Have Changed

- Use of Space and Internet for intelligence, planning, and communications

- Evolution of virtual coalitions
  - Cooperation among previously disparate groups

[redacted]

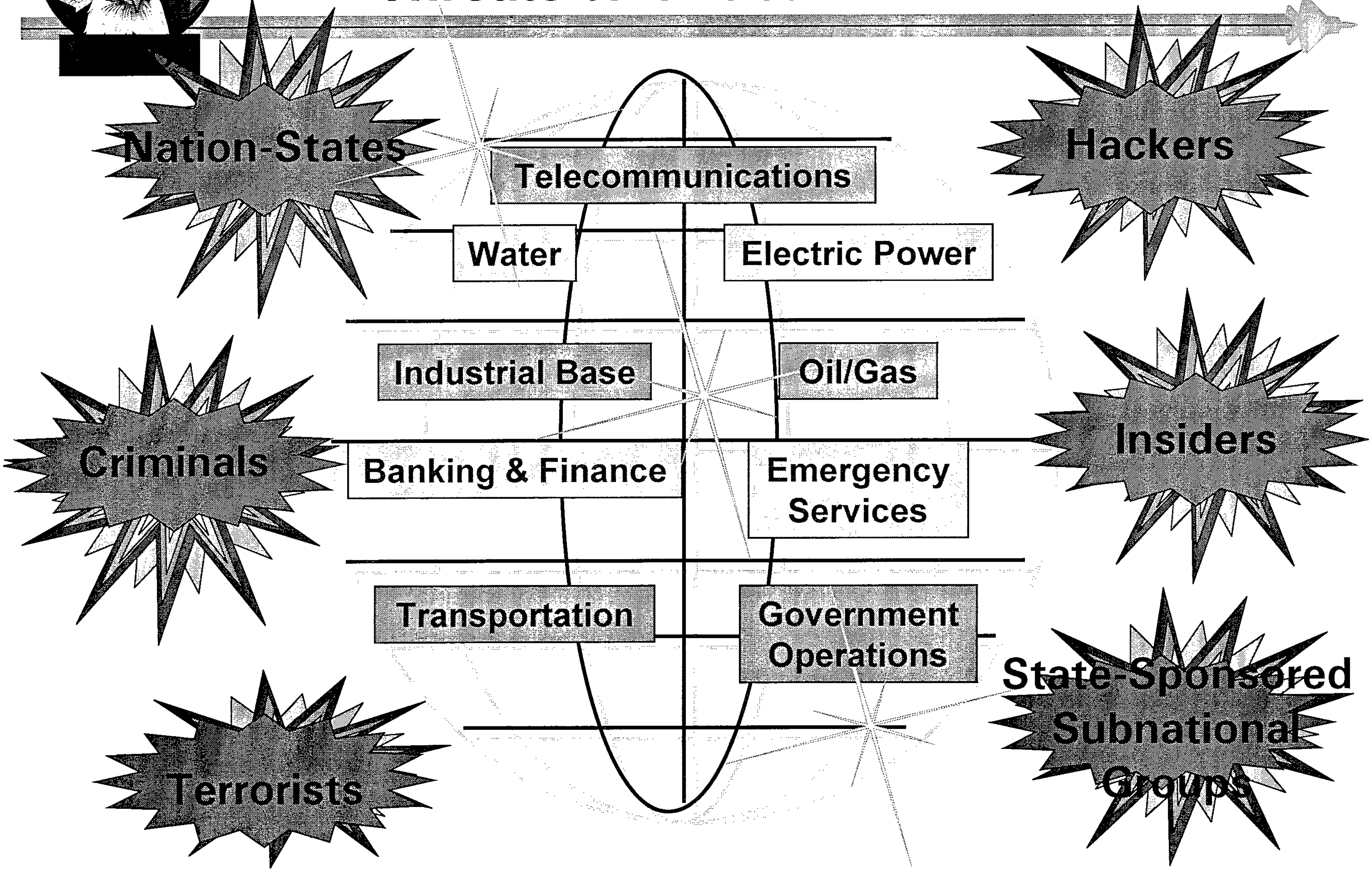
Threat Megatrends

Tools and Methods Have Changed

- Use of Space and Internet for intelligence, planning, and communications
- Evolution of virtual coalitions
- Attacks in cyberspace...direct and indirect
  - Threats to critical infrastructure

Threat Megatrends

Threats to Critical Infrastructure



Nation-States

Hackers

Criminals

Insiders

Terrorists

State-Sponsored Subnational Groups

Telecommunications

Water

Electric Power

Industrial Base

Oil/Gas

Banking & Finance

Emergency Services

Transportation

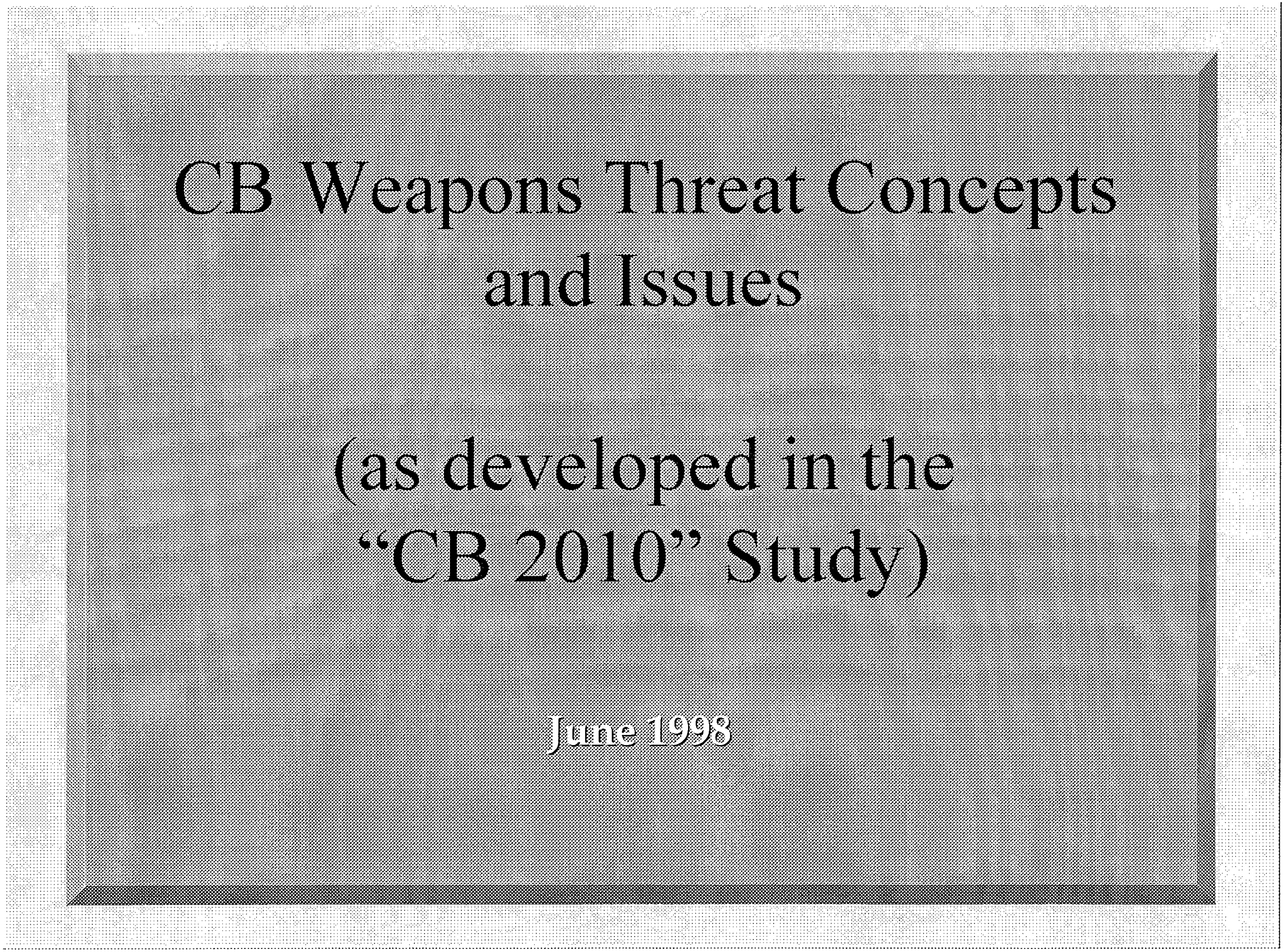
Government Operations

[redacted]

Threat Megatrends

Tools and Methods Have Changed

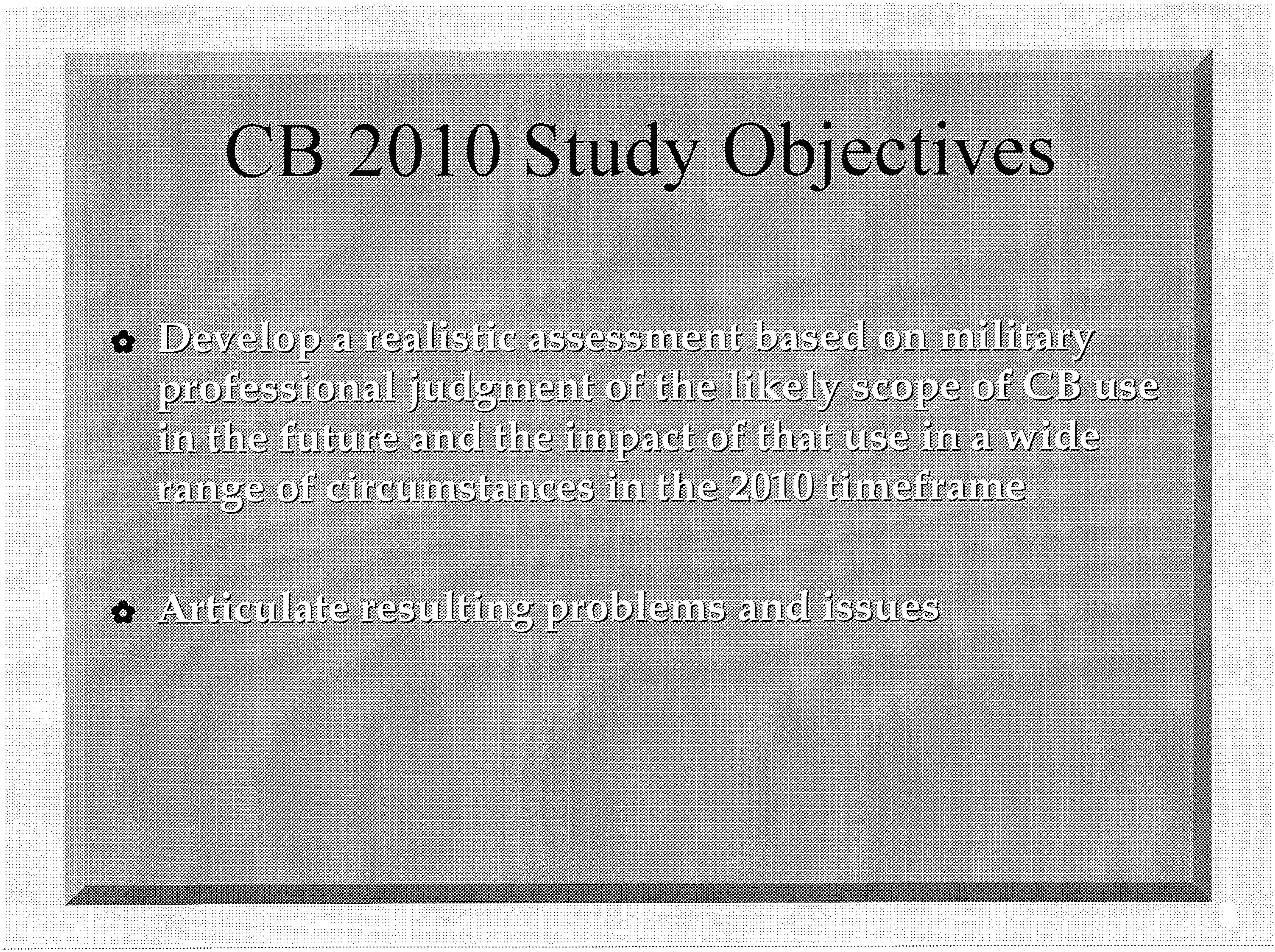
- Use of Space and Internet for intelligence, planning, and communications
- Evolution of virtual coalitions
- Attacks in cyberspace...direct and indirect
- We may well have met an “undeterrable” threat
  - What of value do we hold at risk?
  - Do terrorists want a seat at the table?



CB Weapons Threat Concepts and Issues

(as developed in the "CB 2010" Study)

June 1998



CB 2010 Study Objectives

- Develop a realistic assessment based on military professional judgment of the likely scope of CB use in the future and the impact of that use in a wide range of circumstances in the 2010 timeframe
- Articulate resulting problems and issues

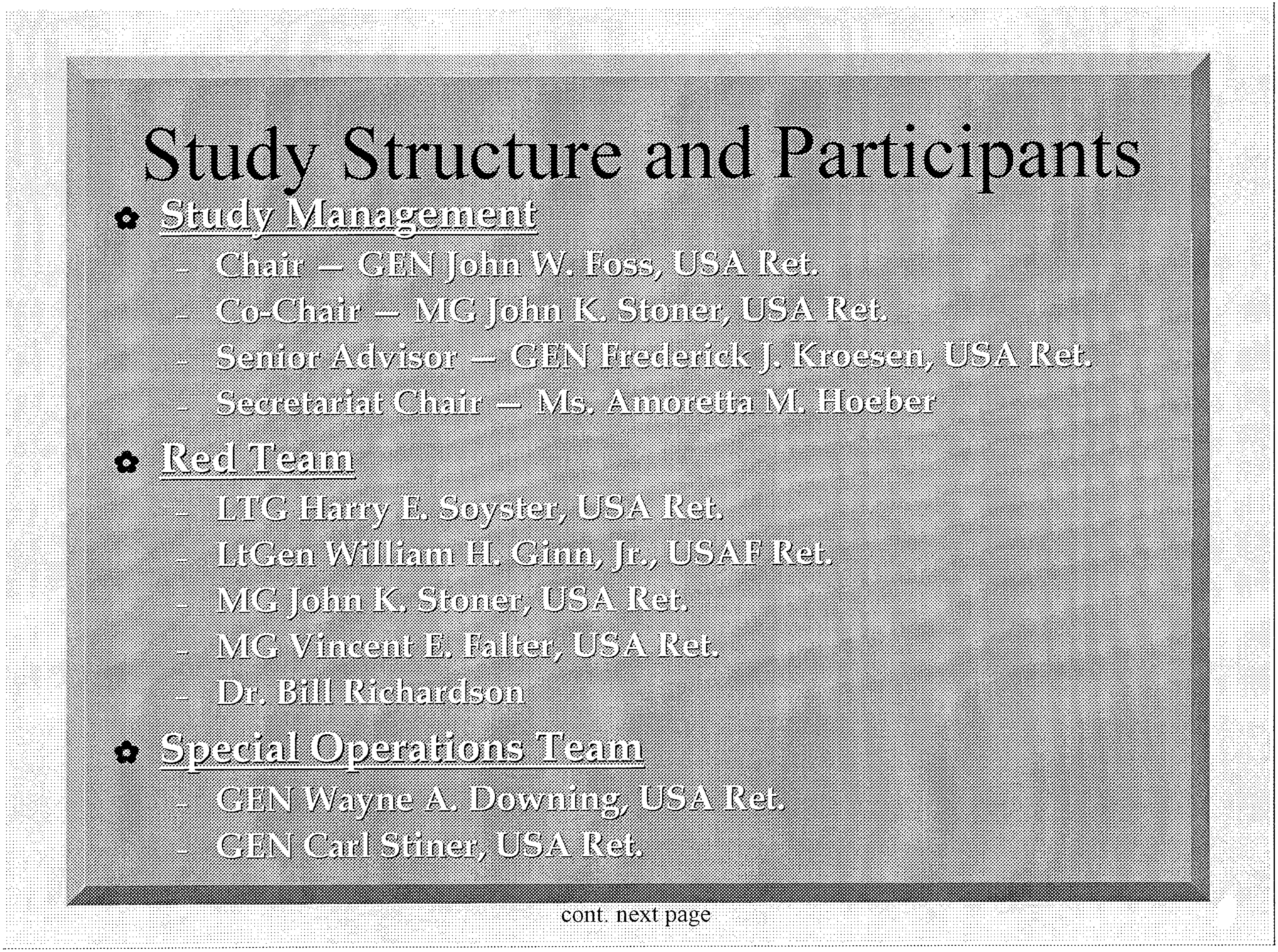
Bottom Line Finding

- This study exposed serious vulnerabilities that could be exploited by the asymmetrical employment of chemical and biological weapons in both CONUS and in the operational theater on our Power Projection System and therefore degrade our nation's ability to respond to crisis

Bottom Line Recommendations

- There must be a significant increase in the level of attention by OSD and the Services to the potential of asymmetrical use of CB weapons.

- The U.S. must develop a capability to deter, counter and prevail in the face of such use of CB weapons



Study Structure and Participants

- **Study Management**
  - Chair — GEN John W. Foss, USA Ret.
  - Co-Chair — MG John K. Stoner, USA Ret.
  - Senior Advisor — GEN Frederick J. Kroesen, USA Ret.
  - Secretariat Chair — Ms. Amoretta M. Hoeber
- **Red Team**
  - LTG Harry E. Soyster, USA Ret.
  - LtGen William H. Ginn, Jr., USAF Ret.
  - MG John K. Stoner, USA Ret.
  - MG Vincent E. Falter, USA Ret.
  - Dr. Bill Richardson
- **Special Operations Team**
  - GEN Wayne A. Downing, USA Ret.
  - GEN Carl Stiner, USA Ret.

cont. next page

Study Structure and Participants
(cont.)

- **Army Team**
  - LTG John J. Yeosock, USA Ret.
  - LTG Dan Schroeder, USA Ret.
  - LTG James H. Johnson, USA Ret.
- **Navy/Marine Corps Team**
  - MG Ray M. Franklin, USMC Ret.
  - MG Jarvis D. Lynch, USMC Ret.
  - RADM Riley Mixson, USN Ret.
- **Air Force Team**
  - LtGen Anthony Burshnick, USAF Ret.
  - LtGen Lawrence E. Boese, USAF Ret.
  - MajGen Hale Burr, USAF Ret.

Study Support

- Office of the Assistant to the Secretary of Defense/Nuclear, Chemical and Biological Counter-proliferation/Chemical and Biological Defense (NCB CP/CBD)
- Office of the Secretary of Defense/Net Assessment
- U.S. Army Chemical and Biological Defense Command (CBDCOM)
- Executive Office, Joint Service Materiel Group

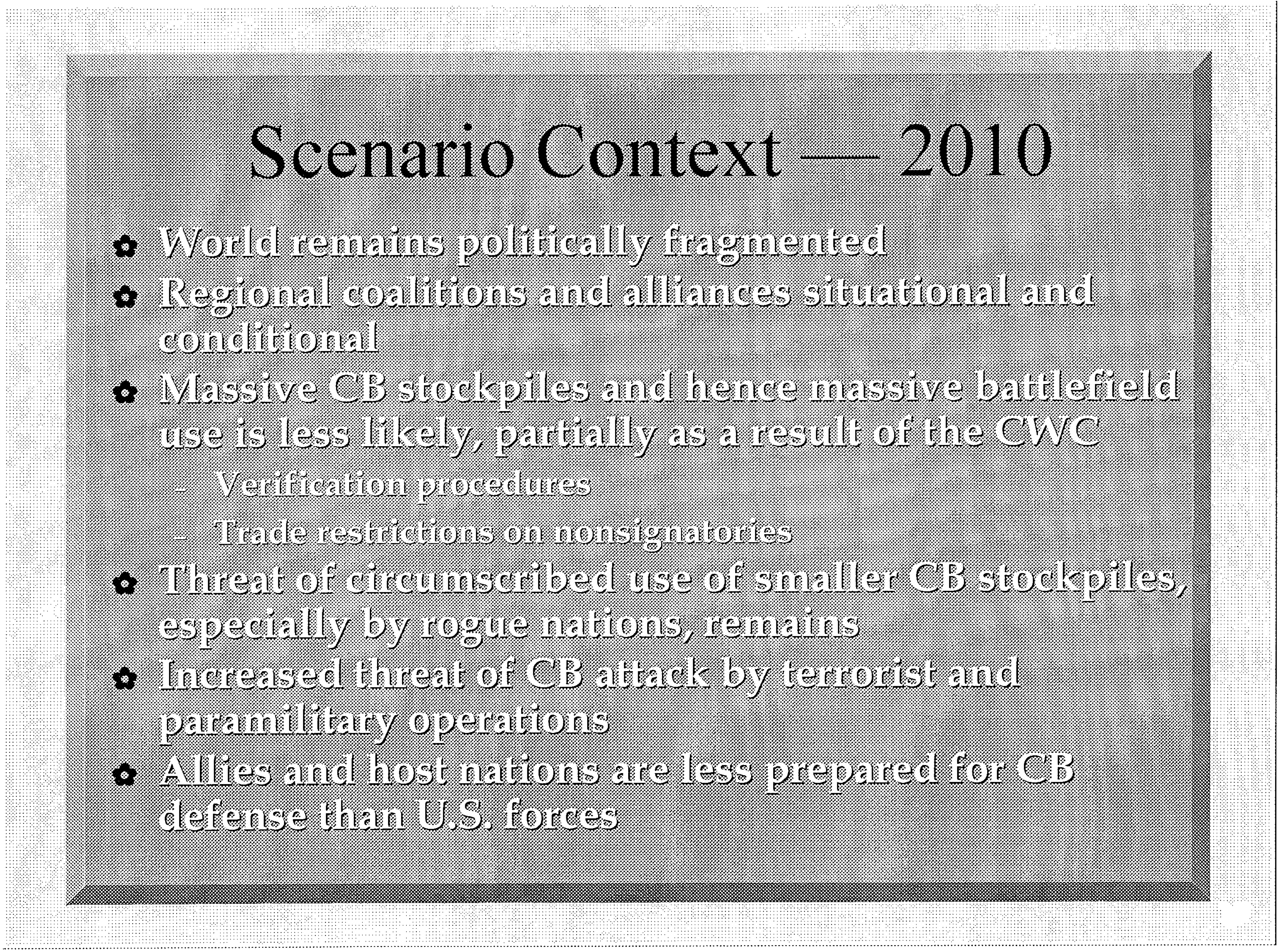
Methodology

- Joint Vision 2010 and Service Visions 2010
  - Requirements to "Project Decisive Force"
  - Use of technology to gain "Full Spectrum Dominance"
  - Little CB consideration
- Briefing updates for Team
  - 2010 intelligence projections
  - Service CB operational concepts and priorities
  - Current and projected U.S. R&D programs
  - Other CB studies underway

cont. next page

Methodology (cont.)

- Development of credible postulated CB use
- Interactive gaming of scenario with and without CB use
- Comparative analysis
- Accumulation of insights from gaming results
- Development of findings and recommendations



Scenario Context — 2010

- World remains politically fragmented
- Regional coalitions and alliances situational and conditional
- Massive CB stockpiles and hence massive battlefield use is less likely, partially as a result of the CWC
  - Verification procedures
  - Trade restrictions on nonsignatories
- Threat of circumscribed use of smaller CB stockpiles, especially by rogue nations, remains
- Increased threat of CB attack by terrorist and paramilitary operations
- Allies and host nations are less prepared for CB defense than U.S. forces

Scenario

- Southwest Asia (Persian Gulf) selected as geographical area
  - Major challenge for U.S. military deployment
  - Scenarios in area well-accepted, with historical baseline
  - Rogue nations possess and are likely to continue to develop CB capabilities
- Potentially hostile nations have assuredly learned the following "lessons" from Desert Storm:
  - Do not allow U.S. (and Allies) to build up massive force
  - Do not allow U.S. to build a coalition
  - Do not try to fight U.S. military strength for strength
  - Neutralize U.S. strengths by asymmetrical means
- These "lessons" can be implemented with small stockpiles of CB weapons

Postulated Threat Concept

- Most effective use of CB is in asymmetrical attacks on U.S. Power Projection System
  - Fear of massive retaliation governs choices
  - Decide to use nonlethal CB to gain advantage but avoid large number of fatalities/casualties and thereby minimize probability of U.S. retaliation

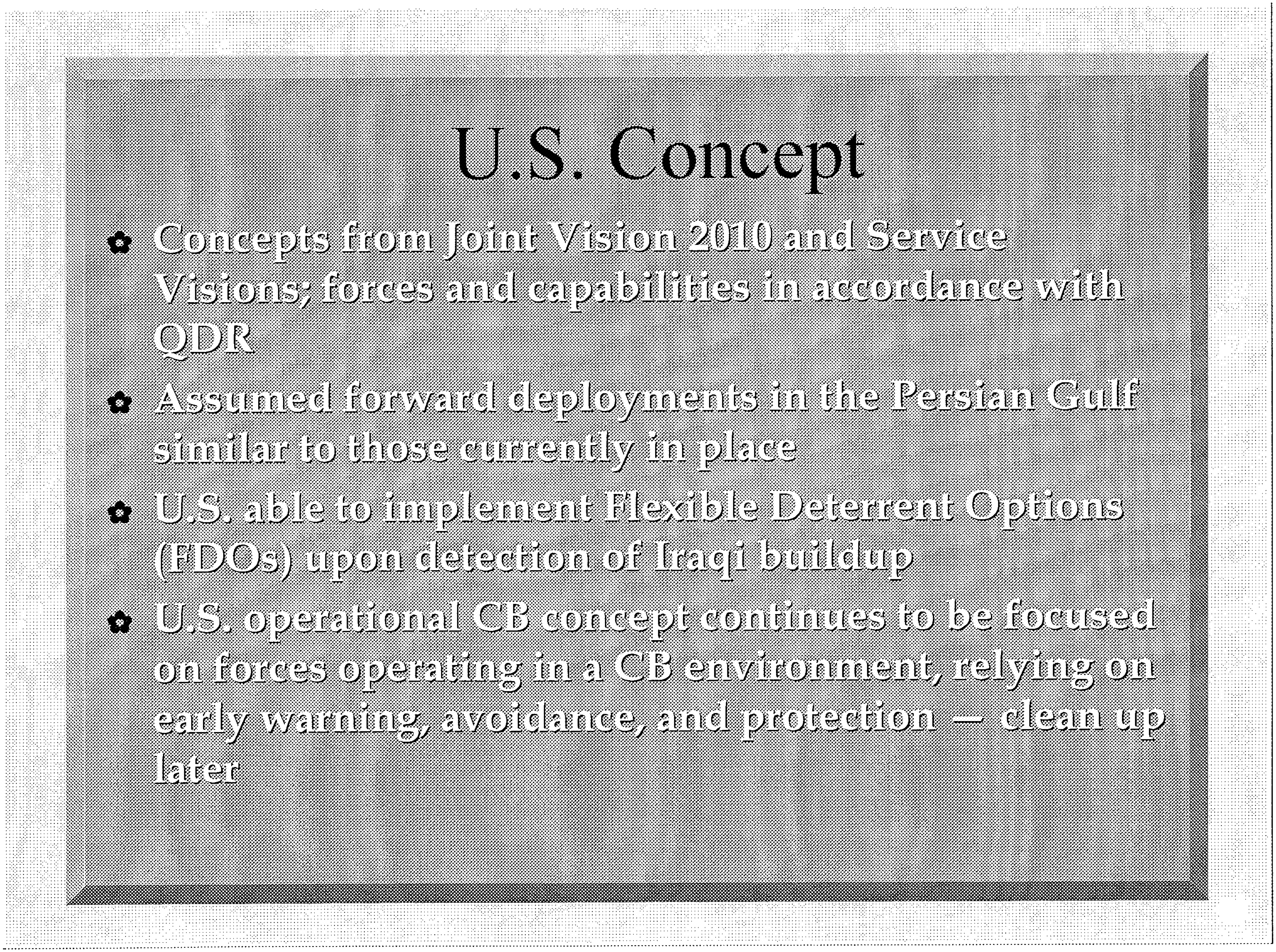
*The scenario postulated in this study has not been "validated" by any official intelligence agency

cont. next page

The Threat in Our Scenario

- Iraq used nonlethal, persistent CB weapons as follows*:
  - BW (cholera) against prepositioned equipment afloat at Diego Garcia (D-3) to delay deployment
  - Persistent CW (mustard) against prepositioned equipment in Kuwait
  - Persistent CW (mustard) to contaminate ports and airbases in Persian Gulf
- Iran used its well-developed terrorist network in U.S. to conduct non-attributable, nonlethal, persistent CW (mustard) attacks on selected deployment airfields and ports in CONUS

*Agents selected for our scenario are examples. There are a variety of available non-lethal and persistent agents that would have equivalent military impact.

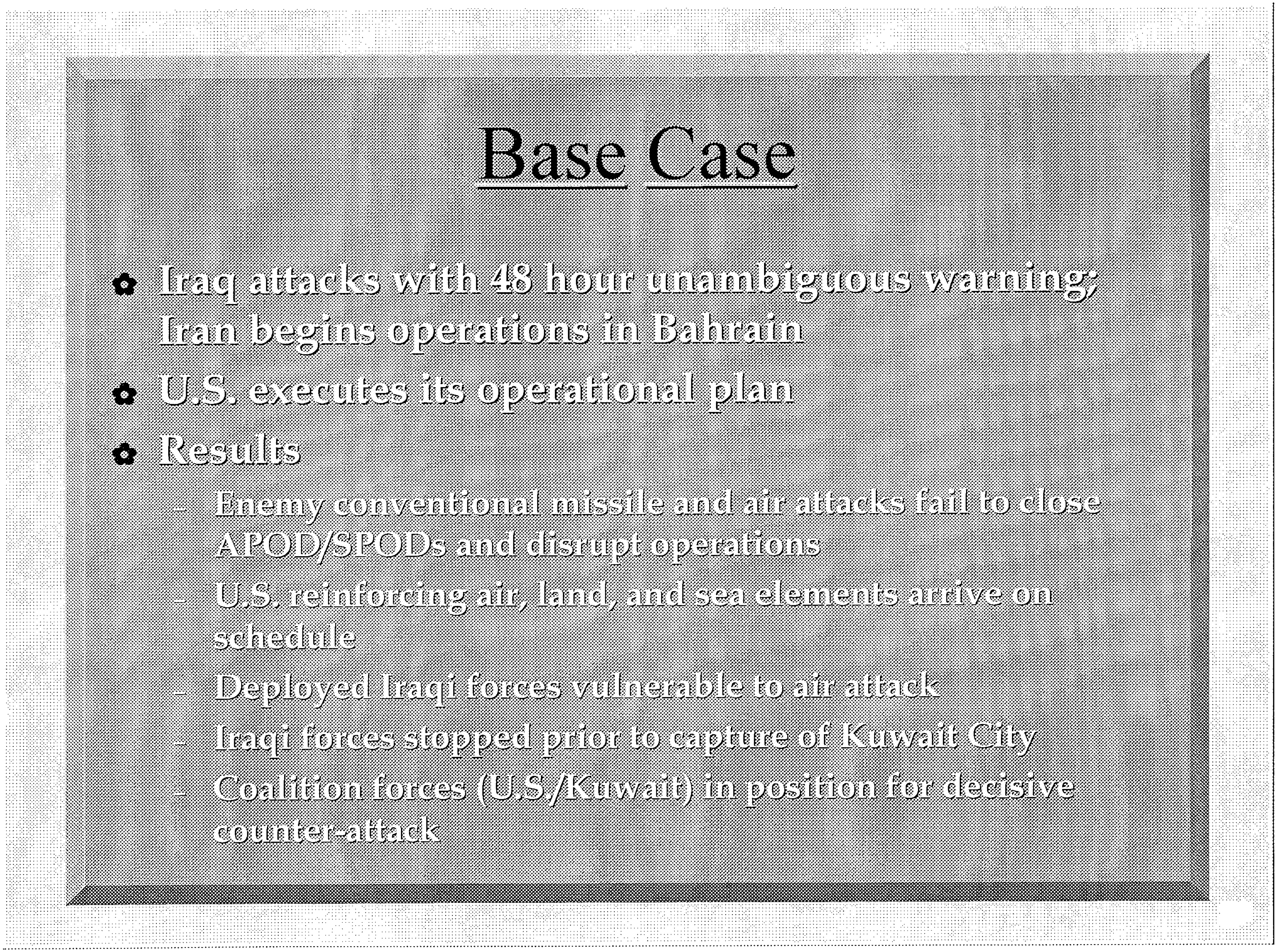


U.S. Concept

- Concepts from Joint Vision 2010 and Service Visions; forces and capabilities in accordance with QDR
- Assumed forward deployments in the Persian Gulf similar to those currently in place
- U.S. able to implement Flexible Deterrent Options (FDOs) upon detection of Iraqi buildup
- U.S. operational CB concept continues to be focused on forces operating in a CB environment, relying on early warning, avoidance, and protection — clean up later

Scenario Gaming

- Base Case – no use of chemical/biological weapons
- CB Case – CB weapons employed per Red Concept
- Comparative analysis of base case and CB case
- Development of findings



Base Case

- Iraq attacks with 48 hour unambiguous warning; Iran begins operations in Bahrain
- U.S. executes its operational plan
- Results
  - Enemy conventional missile and air attacks fail to close APOD/SPODs and disrupt operations
  - U.S. reinforcing air, land, and sea elements arrive on schedule
  - Deployed Iraqi forces vulnerable to air attack
  - Iraqi forces stopped prior to capture of Kuwait City
  - Coalition forces (U.S./Kuwait) in position for decisive counter-attack

CB Case

- Iraq neutralizes MPF (prepositioned afloat for all services, including supplies and equipment for two brigades, one Army and one Marine) at Diego Garcia at D-3
- Nonlethal and unobserved bio attack by single aircraft
  - Crews affected, some equipment contaminated
- Iraq begins operations providing 48-hour unambiguous warning; Iran begins operations in Bahrain
- CINCENT begins FDO with a Brigade (to man Kuwaiti set) and AEF (deploying from Langley, Shaw and Seymour Johnson) on D-2

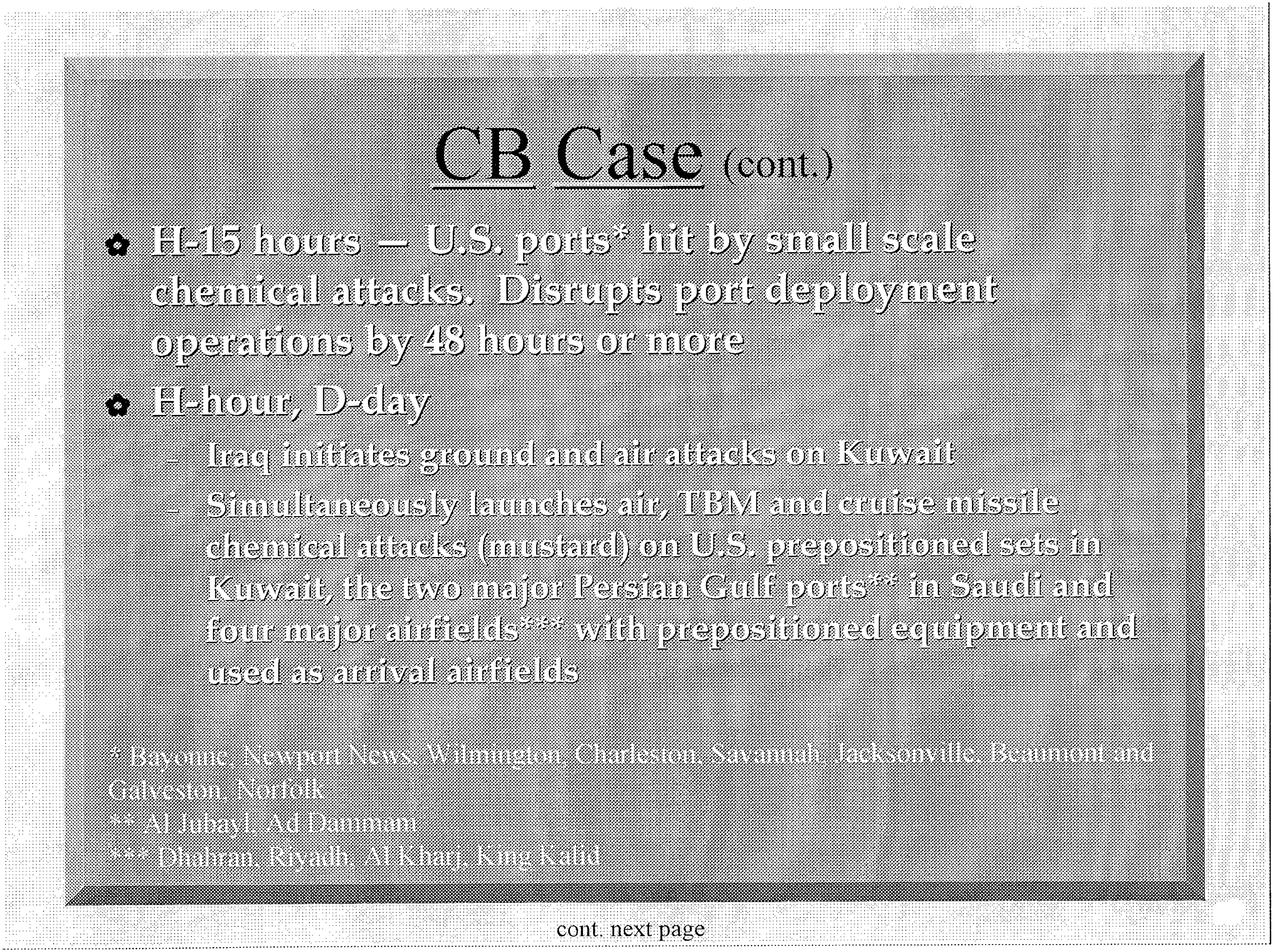
cont. next page

CB Case (cont.)

- President announces U.S. response (at H-44 hours)
- Chemical attacks (mustard) implemented at H-39 hours at ten U.S. APOEs* via unconventional means (crop dusters, fuel trucks, etc.)
- These attacks disrupt FDO deployment of brigade (3ID) and AEF. Army transfers deployments to other airfields. AF alerts and begins deployment of later assets. A minimum of 24 hours delay in airlift, 48 or more hours in cleanup

* Hunter AAF, Robt. Gray AAF, Pope/(Ft. Bragg) AFB, Ft. Campbell AAF, Dover AFB, Langley AFB, Seymour Johnson AFB, McGuire AFB, Barksdale AFB and Charleston AFB

cont. next page



CB Case (cont.)

- H-15 hours — U.S. ports* hit by small scale chemical attacks. Disrupts port deployment operations by 48 hours or more
- H-hour, D-day
  - Iraq initiates ground and air attacks on Kuwait
  - Simultaneously launches air, TBM and cruise missile chemical attacks (mustard) on U.S. prepositioned sets in Kuwait, the two major Persian Gulf ports** in Saudi and four major airfields*** with prepositioned equipment and used as arrival airfields

* Bayonne, Newport News, Wilmington, Charleston, Savannah, Jacksonville, Beaumont and Galveston, Norfolk
** Al Jubayl, Ad Dammam
*** Dhahran, Riyadh, Al Kharj, King Kalid

cont. next page

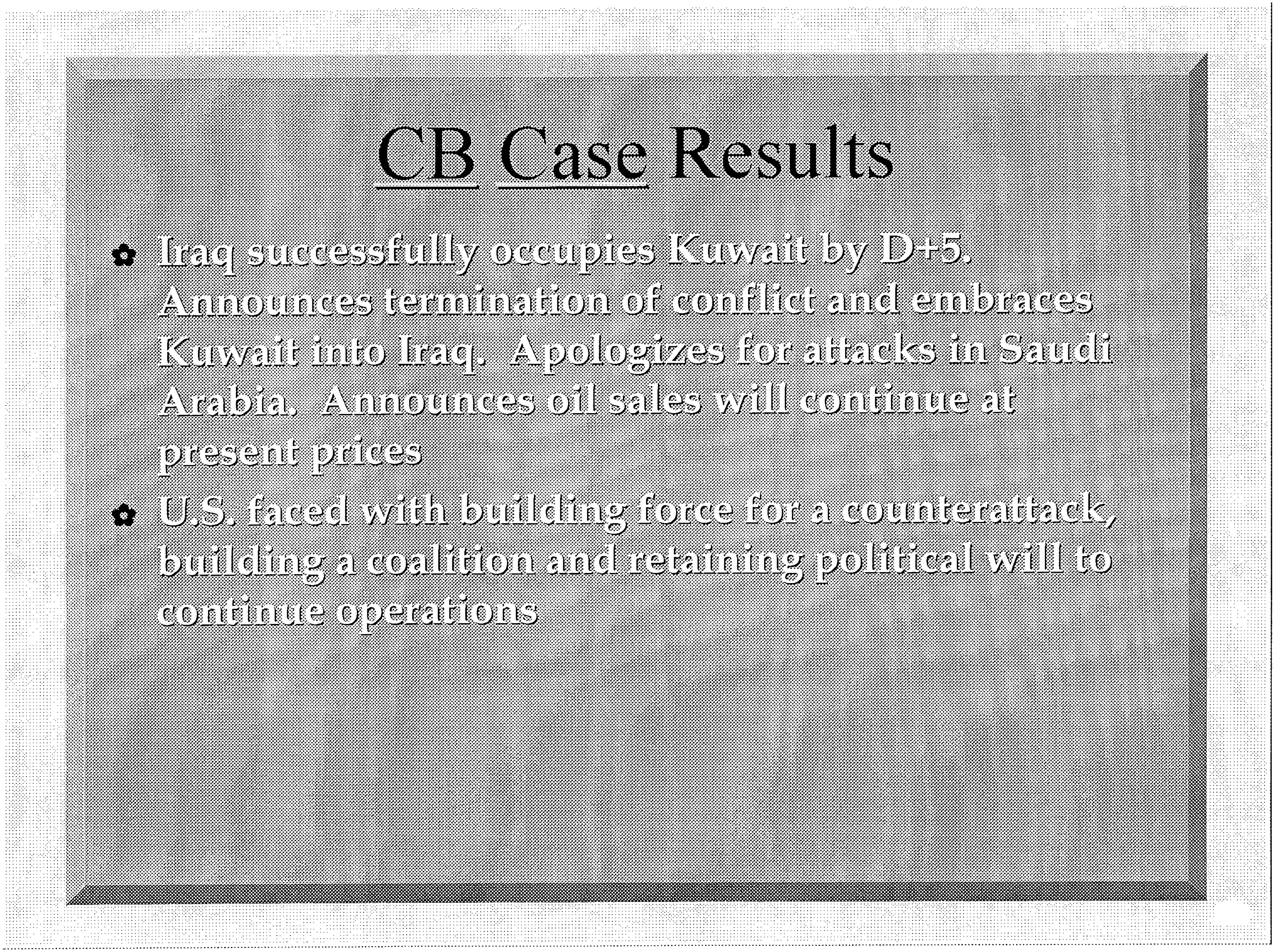
CB Case (cont.)

- Army brigade in Kuwait only partially deployed upon attack
  - Withdraws most equipment to Saudi Arabia
  - Joined by MEU to provide defense of Saudi
- U.S. air combat operations greatly disrupted by cleanup and impact of MOPP and by relocation of operations to alternative airfields
- Civil Air declines to operate from "dirty" airfields
- Force arrivals shifted to Western Saudi airfields.
- Buildup requires in-country decontamination and extensive motor transportation

cont. next page

CB Case (cont.)

- U.S. force generation activities and operational capabilities severely curtailed during early stages of operations; Air priority to air defense in Saudi; interdiction attacks primarily limited to use of Naval air and cruise missiles, and USAF B-1 and B-2 attacks on Iraqi targets
- D+2 — Terrorist chemical attack (mustard) on Pentagon Metro Station after night closing
  - Escalator contaminated; station closed
  - Results in heightened security and cleanup, disrupting Washington, D.C. activities



CB Case Results

- Iraq successfully occupies Kuwait by D+5. Announces termination of conflict and embraces Kuwait into Iraq. Apologizes for attacks in Saudi Arabia. Announces oil sales will continue at present prices
- U.S. faced with building force for a counterattack, building a coalition and retaining political will to continue operations

Conclusion

- Asymmetrical employment of chemical and biological weapons in CONUS and the operational theater can exploit vulnerabilities in our Power Projection System which could have serious impact on our nation's response to a crisis

Threat Finding

- **Finding #1: Massive use of chemical weapons on the battlefield appears less likely in 2010 because:**
  - The Chemical Weapons Convention will make manufacturing, weaponizing and delivering large quantities of chemical weapons more difficult
  - The relative importance of massive forces facing each other in static confrontations will be less
  - U.S. forces will be perceived as able to fight protected, given the capabilities of our battlefield-oriented protective equipment
  - The use of chemical and biological weapons by terrorists or small "special operations" teams is not reduced and may even be increased by these same factors

cont. next page

Threat (cont.)

- Recommendations: OSD and Service planners and policy makers should explicitly address in all future posture assessments achieving a capability to deal with increased threats of CB use, including:
- CB use against U.S. forces at CONUS bases prior to or during operational deployment
  - CB use against intermediate staging bases
  - CB use against bases in theater
  - CB terrorism against U.S.(CONUS) targets
- Avoid any CWC-induced complacency and address the growing terrorist and asymmetrical use threats of CB

Focus Finding

- Finding #2: Current Service doctrine and operational concepts are focused on massive use of chemicals on the battlefield. This focus has driven the operational concepts and requirements and hence RDA.
- "Operate through" was an appropriate concept of the Cold War, but is less appropriate concept today
  - Lower intensity conflicts, such as we have today and will have in the next decade, are dependent upon force projection and support from friendly nations
  - Protection of the force projection facilities and capabilities is necessary

cont. next page

Focus (cont.)

- Recommendation: Services should expand doctrine and operational concepts to include other than massive battlefield uses of CB:
  - Joint Force and Service doctrine and operational concepts should be broadened specifically to deal with use of CB by terrorists and small teams
  - Expanded concepts should be used in RDA prioritization

Intelligence Finding

- Finding #3: Intelligence deficiencies exist in
  - Determining intentions and capabilities to use CB weapons
  - Locating small chemical and biological manufacturing and storage sites
  - Identifying pre-launch locations of CB weapons
  - Detecting presence of covert, clandestine and paramilitary capabilities in the theater of operations and in CONUS

cont. next page

Intelligence (cont.)

- Recommendations: Intelligence agencies should expand HUMINT and collection systems specifically targeted at CB capabilities
  - Production and storage
  - Weapons locations
  - Intentions
  - Clandestine capabilities
- The number of analysts addressing CB threats <u>and</u> the level of CB awareness of analysts focusing on other threats must be increased

Deterrence Finding

- Finding #4: Established concepts of deterrence and retaliation do not consider CB use by terrorists or small action teams against the Power Projection System followed by denial of action
- Recommendation: Deterrence and retaliation policies should be broadened to reflect the current world threat environment (the DSWA deterrence model offers a useful method to address some of these issues)

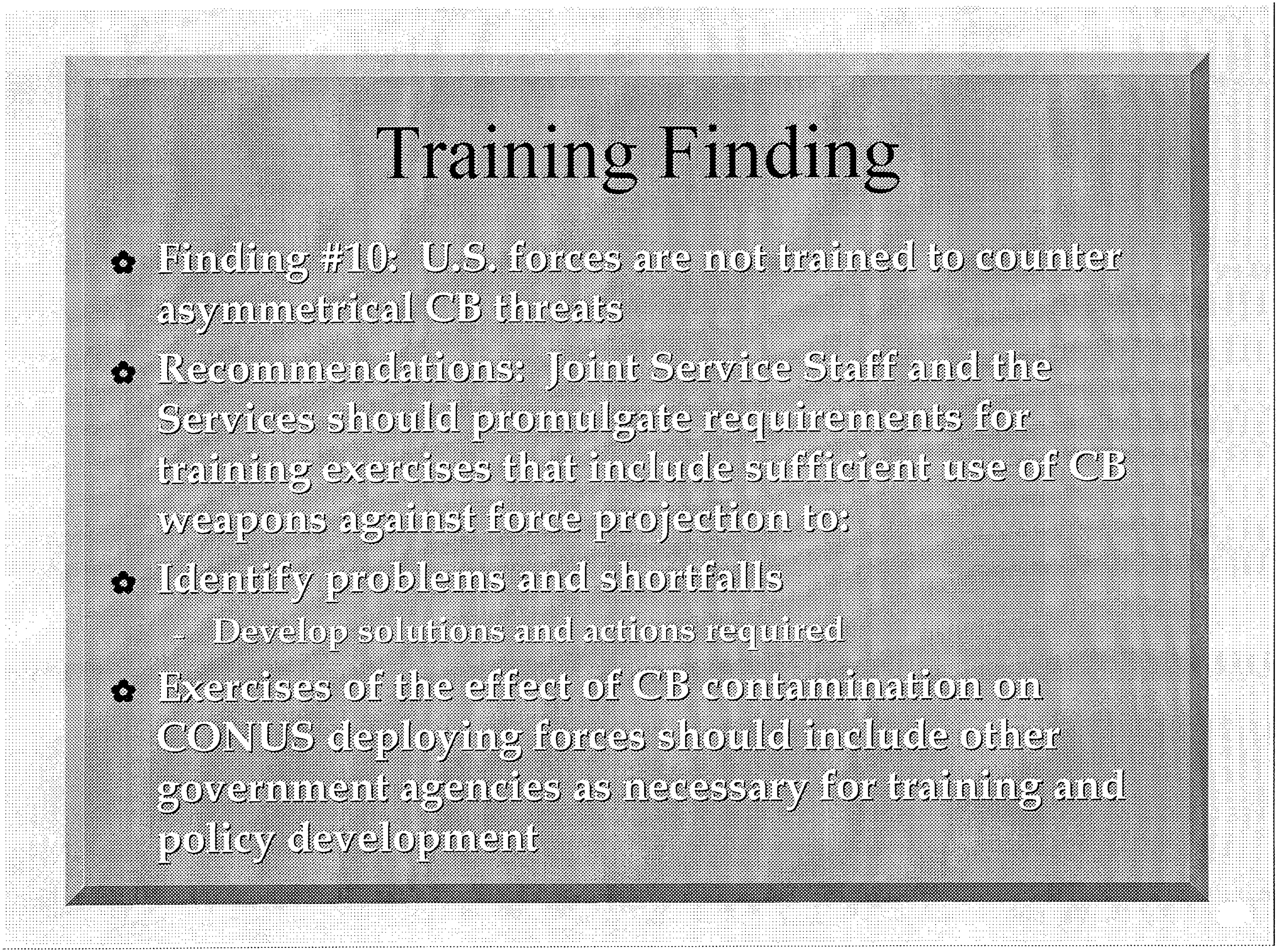
CONUS Sanctuary Status Finding

- Finding #5: CONUS, especially APOEs/SPOEs, can no longer be considered immune to attack, especially CB attack, during the operational deployments of forces
- There have been several terrorist attacks in the U.S. in recent years
  - Employment of CB weapons against CONUS facilities has major impact and is hence attractive to an opponent
  - Asymmetrical attacks of all types (including CB) in CONUS could be executed in support of overseas operations

cont. next page

CONUS Sanctuary Status (cont.)

- Recommendation: Additional force structure, training and equipment are required. Force protection concepts, R&D, and resource allocations should be balanced to address CONUS as well as OCONUS facilities and requirements



Training Finding

- Finding #10: U.S. forces are not trained to counter asymmetrical CB threats
- Recommendations: Joint Service Staff and the Services should promulgate requirements for training exercises that include sufficient use of CB weapons against force projection to:
- Identify problems and shortfalls
  - Develop solutions and actions required
- Exercises of the effect of CB contamination on CONUS deploying forces should include other government agencies as necessary for training and policy development

Civilian, Contractor and Host Nation Support Personnel Finding

- Finding #11: Increased reliance on civilian employees and contractor and host nation personnel, all of whom are currently unprotected against CB, is an increasing vulnerability
- Recommendations: U.S. forces, civilian employees, and contractor personnel should be equipped and trained to the level of protection against CB required for those forces they support
- Materiel to achieve this objective should be included in future requirements

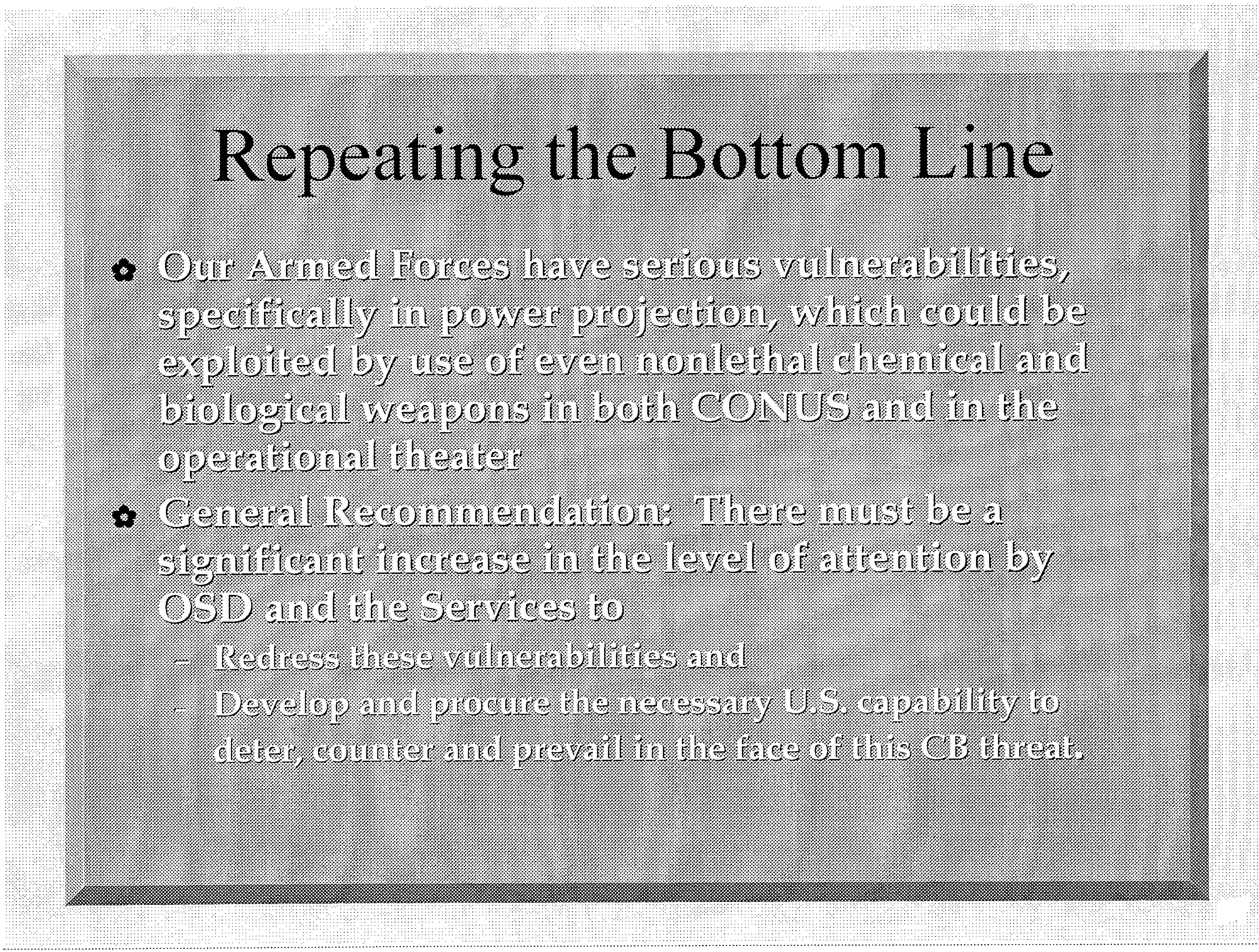
cont. next page

Civilian, Contractor and Host Nation Support Personnel (cont.)

- U.S. equipment and capabilities should be marketed internationally to realize economies of scale and strengthen regional coalition

Public Reaction Finding

- Finding #12: We could not estimate the likely public reaction to chemical attacks on APOEs/SPOEs relative to the availability of the civilian/contractor workforce to support deploying forces
- Special Recommendation: OSD should focus attention on the problems of potential CB attack on CONUS military facilities. We believe that rapid decontamination to high levels of assurance will be vital to bringing the workforce back quickly after attack



Repeating the Bottom Line

- Our Armed Forces have serious vulnerabilities, specifically in power projection, which could be exploited by use of even nonlethal chemical and biological weapons in both CONUS and in the operational theater
- General Recommendation: There must be a significant increase in the level of attention by OSD and the Services to
  - Redress these vulnerabilities and
  - Develop and procure the necessary U.S. capability to deter, counter and prevail in the face of this CB threat.

Final Conclusion

- Given the right level of attention, funding and leadership by OSD, Joint Commanders and the Services, it is believed that this problem can be <u>reduced to manageable size</u>

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
OFFICE OF SCIENCE AND TECHNOLOGY POLICY

CRITICAL INFRASTRUCTURE PROTECTION:

DEVELOPING THE FEDERAL R&D AGENDA

Dr. Steven M. Rinaldi
Office of Science and Technology Policy

June 16, 1998

A STRONG CALL FOR R&D

- **The President's Commission called out R&D for particular emphasis**
  - **Recommended $4.75 billion investment (FY98-FY04)**
  - **Increased focus in six areas:**
    - ➢ **Information assurance**
    - ➢ **Intrusion detection and monitoring**
    - ➢ **Vulnerability assessment and systems analysis**
    - ➢ **Risk management decision support**
    - ➢ **Protection and mitigation**
    - ➢ **Incident response and recovery**

- **The Commission stressed the importance of a strong government - private sector - academia partnership**

THE PRESIDENT'S RESPONSE

THE POLICY DECISION:

"It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."

White Paper on PDD-63, May 22, 1998

THE PRESIDENT'S RESPONSE

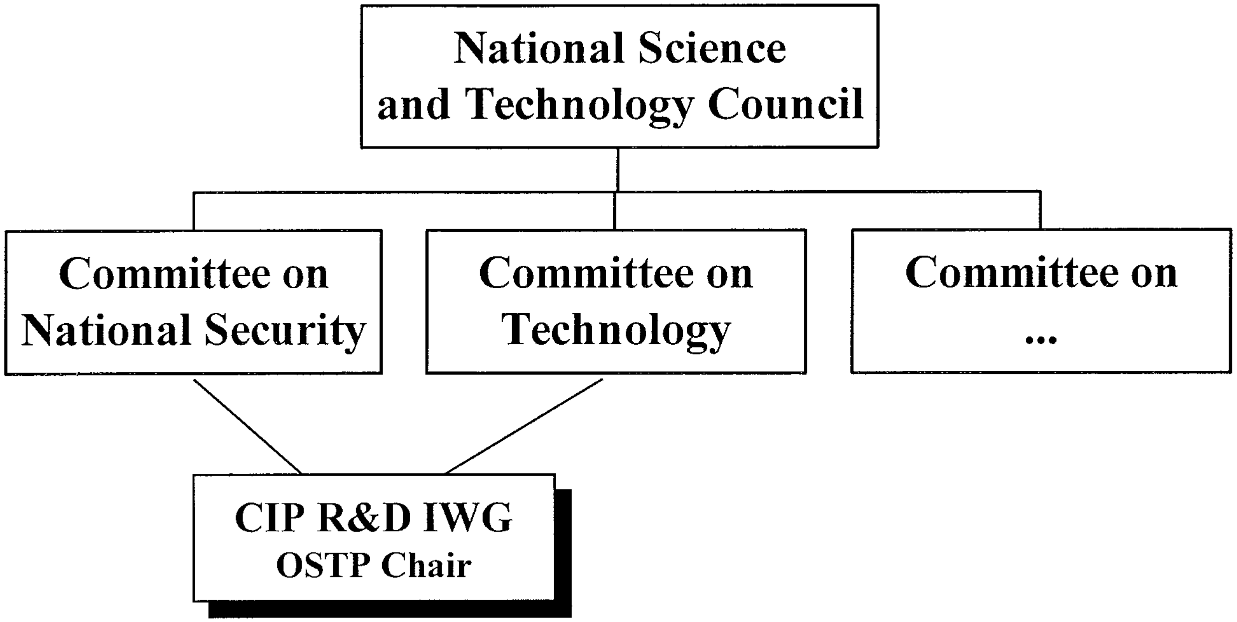
OUR R&D TASKING:

"Research and Development: Federally-sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable."

White Paper on PDD-63, May 22, 1998

THE PRESIDENT'S RESPONSE

- **Interagency coordination is key**
- **PDD-63 direction: "OSTP shall be responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council."**



National Science and Technology Council

Committee on National Security

Committee on Technology

Committee on ...

CIP R&D IWG
OSTP Chair

UP AND RUNNING

- **Interagency Working Group established in March**
- **Goals:**
  - **Develop and coordinate the federal government's critical infrastructure protection R&D agenda before end of year**
  - **Provide early version of the agenda to the Critical Infrastructure Coordination Group by late July**
  - **Reach out to industry, academia, and international partners**
- **PDD-63 deadline - deliver plan to the President by mid-November**

CURRENT ACTIVITIES

- Activities are well underway to achieve these goals
  - Identifying ongoing agency programs and budgets
  - Summarizing infrastructure vulnerabilities, drawing upon analyses in other studies (e.g., PCCIP report, Argonne National Laboratory, Department of Transportation)
  - Will develop near/long term budget recommendations and plan

- PCCIP Transition Office roadmapping study
  - Involved government, private sector, academia, and national labs
  - Focused on perceived technology gaps between infrastructure protection needs and available technologies
  - Recommended R&D programs to address the gaps

Critical Infrastructure Protection R&D
Interagency Working Group

20 PLAYERS

Arms Control and Disarmament Agency
Central Intelligence Agency
Department of Commerce
Department of Defense
Department of Energy
Department of Health and Human Services
Department of the Interior
Department of State
Department of Transportation
Department of the Treasury
Environmental Protection Agency
Federal Bureau of Investigation
Federal Emergency Management Agency
National Aeronautics and Space Agency
National Institute of Occupational Safety and Health
National Security Agency
National Security Council
National Science Foundation
Office of Management and Budget
Office of Science and Technology Policy

Critical Infrastructure Protection R&D
Interagency Working Group

SHARING THE LOAD

SUBGROUPS	***AGENCIES***
• **Banking and Finance**	**Treasury (lead), DOJ, DOS, DOC, FED**
• **Information and Comm**	**DOC (lead), DOD, DOJ, NSF**
• **Transportation**	**DOT (lead), NASA, DOE**
• **Energy**	**DOE (lead), DOI**
• **Vital Human Services**	**HHS (lead), EPA, FEMA, NIH, PHS, DOI, DOE**
• **Budget**	**OMB (lead), DOD**
• **Outreach**	**DOC (lead), NSF, DOS, ACDA, DOD DOT, DOE**
• **Interdependencies**	**OSTP (lead), DOD, DOC, Treasury, DOT, DOE, HHS, OMB**

OUTREACH - PARTNERSHIP

White Paper on PDD-63: "...the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative."

- **OSTP and other agencies recognized early on the importance of partnerships with industry and academia and are committed to fostering them**
- **IWG has established an outreach subgroup chaired by Commerce**
- **Initial contacts with industry:**
  - **Close contact with NSTAC and its member companies**
  - **Participation in symposia: Armed Forces Communications and Electronics Association, National Defense Industrial Association**

SUMMARY

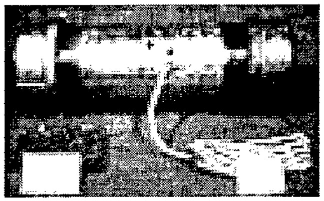
- IWG established to develop and coordinate federal government's critical infrastructure protection R&D agenda
- IWG activities well underway
- Partnership with the private sector, academia, and international partners is key to success

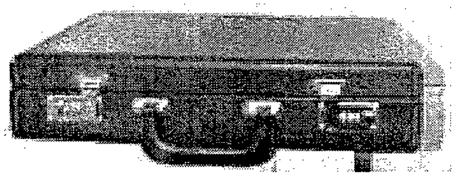
Addressing the Threat During Project Execution:
The U.S. Blast Mitigation Program

14th Annual Security Technology Symposium & Exhibition
Williamsburg, Virginia, 16 June 1998
Presented by: Mr. Douglas A. Sunshine, PMT/DSWA

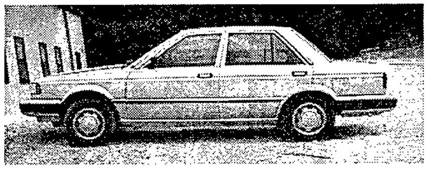
Define Threat

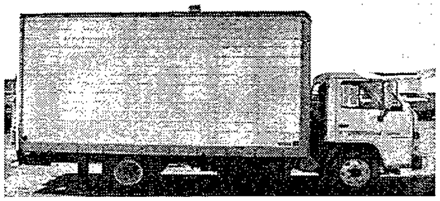
- **Range of threats considered**
  - Mail/Briefcase bomb





  - Vehicle bomb

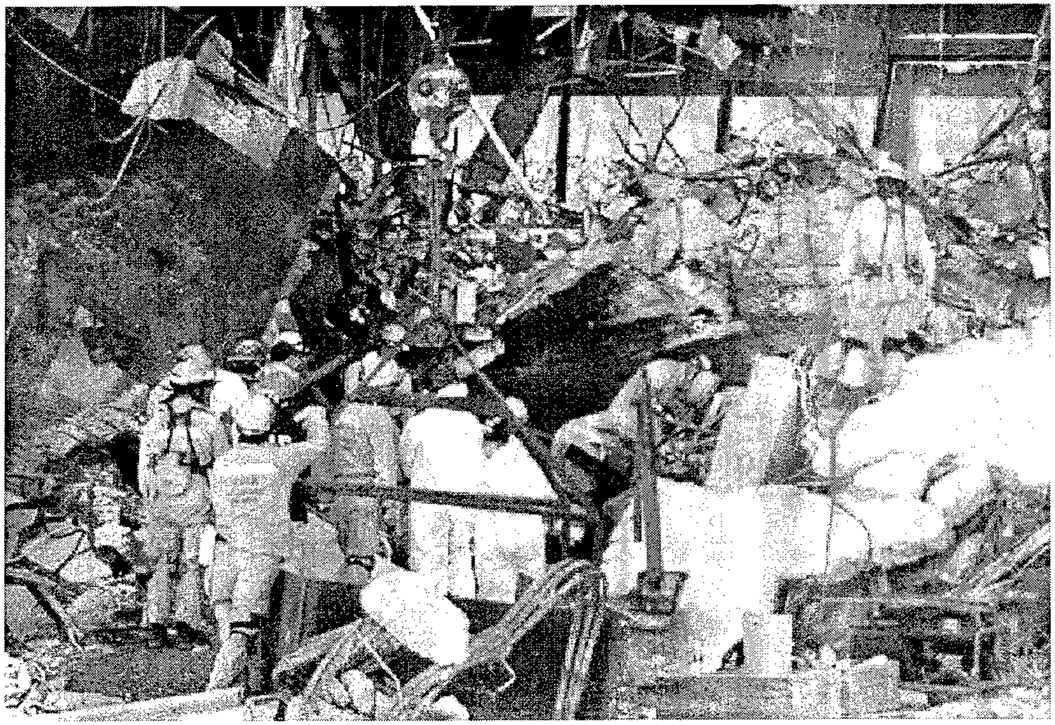




- **Exact threat is difficult to predict**
  - Size and type of bomb
  - Distance from target

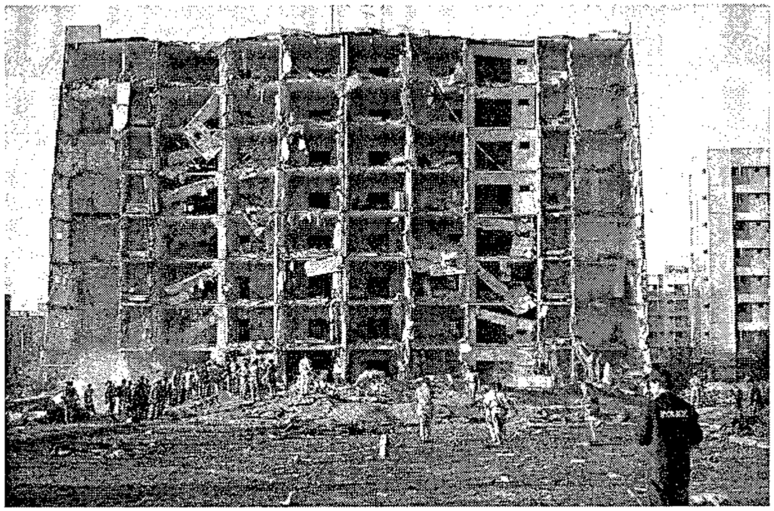
Consequences of Attack

- Structural Damage
- Property Damage
- Human Injury



Key Issues

- Structural Collapse
- Flying Debris



End Products

<u>Vulnerability Analysis/Assessment Tools</u>

- Blast Effects Methodologies
- Structural Response Methodologies
- Human Injury Models

<u>Solutions - Design Guidance</u>

- Both New Construction and Retrofits
- Cost - Effective
- Quick & Easy to Install
- Both Permanent & Temporary
- Aesthetically Pleasing

Program Elements

- Evaluate State-of-Knowledge
- Identify and Evaluate Potential Products and Technologies
- Conduct Development and Testing Program
- Develop Final Product with User Involvement

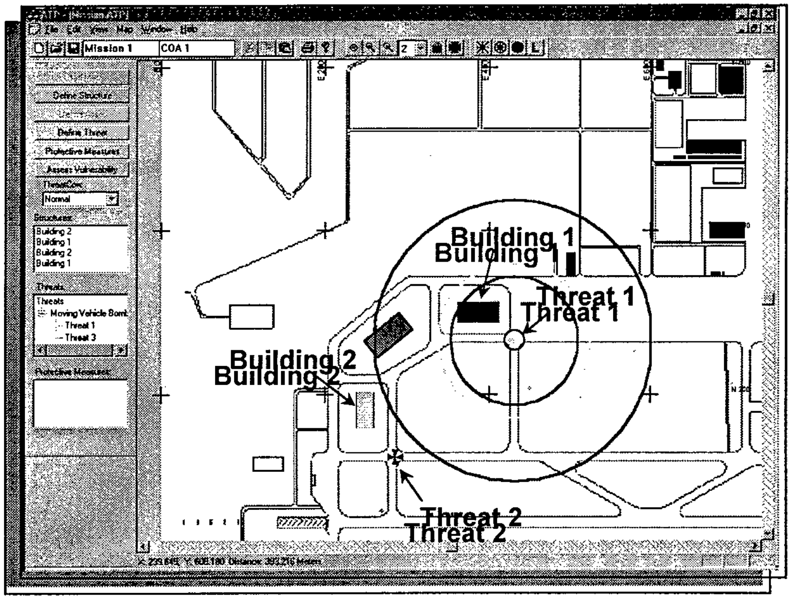
Product Issues

- **Know Your Users**
  - Get users involved in product development
  - Get peer review
- **Develop Variety of Solutions**
  - Cost/Performance Tradeoffs
  - Risk Assessments
- **Develop Dissemination Plan**
  - Military
  - Civilian

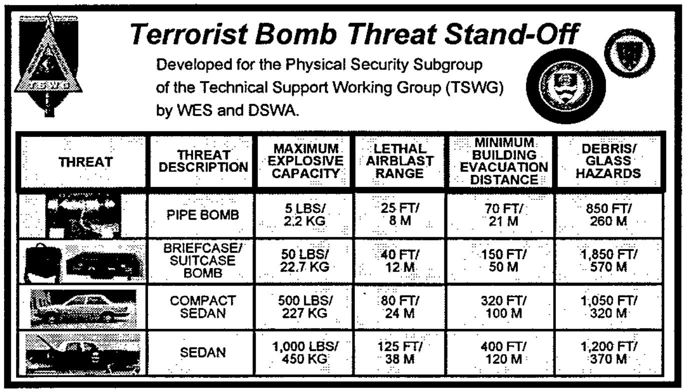
Vulnerability Assessment Tools

- **User-Friendly 80% Solution**
- **Variety of Users - Variety of Tools**
  - Simple Tables
  - Detailed Design/Analysis Computer Software

AT Planner



Bomb Stand-Off Card



Terrorist Bomb Threat Stand-Off

Developed for the Physical Security Subgroup of the Technical Support Working Group (TSWG) by WES and DSWA.

THREAT	THREAT DESCRIPTION	MAXIMUM EXPLOSIVE CAPACITY	LETHAL AIRBLAST RANGE	MINIMUM BUILDING EVACUATION DISTANCE	DEBRIS/ GLASS HAZARDS
	PIPE BOMB	5 LBS/ 2.2 KG	25 FT/ 8 M	70 FT/ 21 M	850 FT/ 260 M
	BRIEFCASE/ SUITCASE BOMB	50 LBS/ 22.7 KG	40 FT/ 12 M	150 FT/ 50 M	1,850 FT/ 570 M
	COMPACT SEDAN	500 LBS/ 227 KG	80 FT/ 24 M	320 FT/ 100 M	1,050 FT/ 320 M
	SEDAN	1,000 LBS/ 450 KG	125 FT/ 38 M	400 FT/ 120 M	1,200 FT/ 370 M

Vulnerability Assessment Tables

Reinforced Concrete

Distance for Specified Damage

Charge Weight (lbs)	Minimal Damage	Minor Damage	Moderate Damage	Heavy Damage	Severe Damage
50	90	38	10	-	-
220	210	100	78	35	-
500	360	175	130	55	32
1000	520	245	195	105	45
4000	1120	570	460	255	110
40000	3000	1900	1500	1010	440

PROTECTS

(Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism in Subways)

National Labs Coordinator:
Dr. Anthony J. Policastro
Argonne National Laboratory
Argonne, Illinois 60439
Ph: (630) 252-3235
Fax: (630) 252-3194
Email: policastro@anl.gov

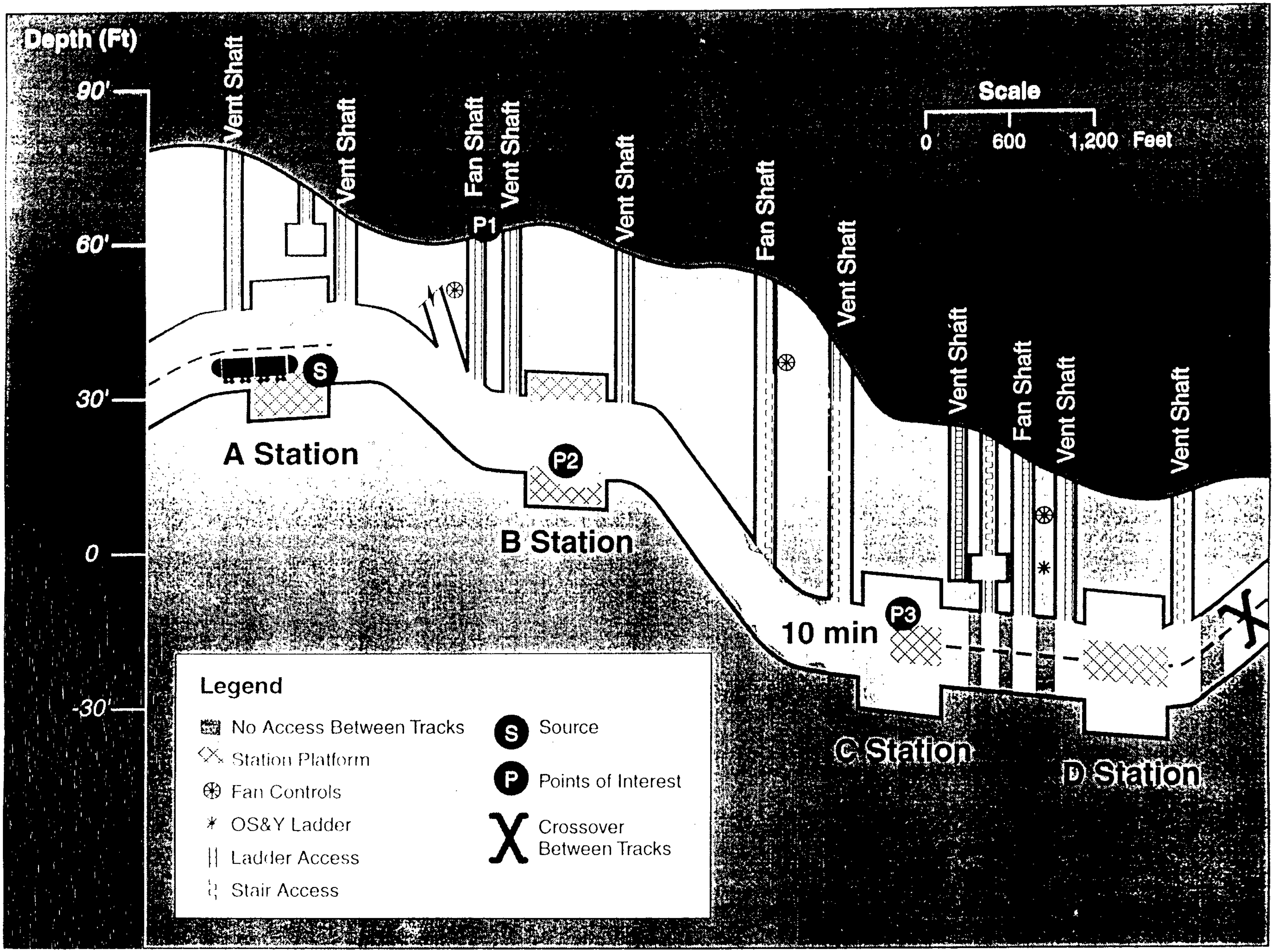
Sponsor:
Dr. Page Stoutland
Chemical/Biological
Nonproliferation Program
U.S. Department of Energy
Washington, D.C. 20585
Ph: (202) 586-2711
Fax: (202) 586-2755
Email: page.stoutland@hq.doe.gov

FTA Coordinator:
Ms. Rhonda Crawley
Office of Technology
Federal Transit Administration
Washington, D.C. 20590
Ph: (202) 366-4035
Fax: (202) 366-3765
Email: Rhonda.Crawley@fta.dot.gov

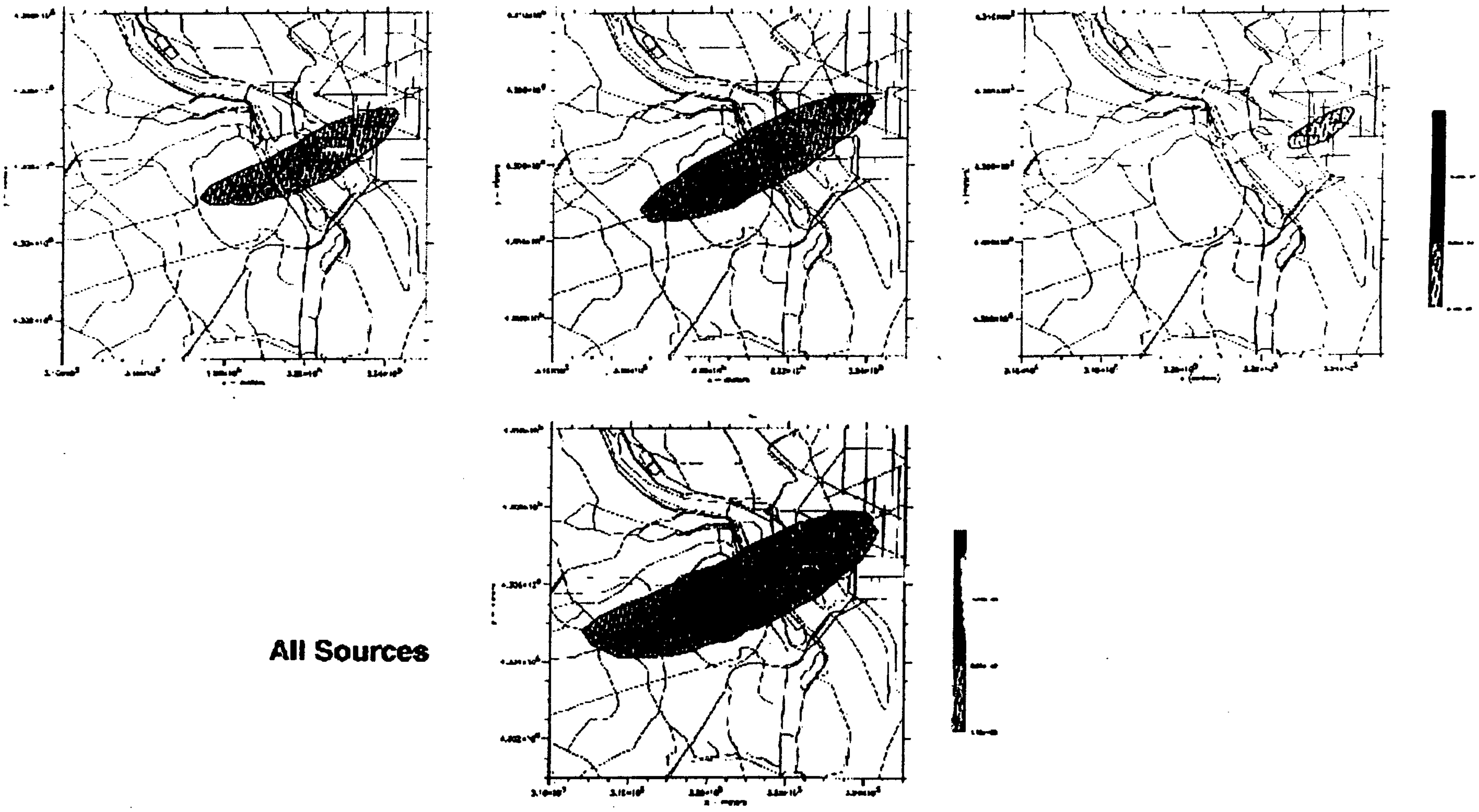
Mineta Report Conclusions

- Terrorists have easy access to public surface transportation, but minimizing casualties and damage and quickly reestablishing service restores the confidence of the public.
- Advance planning is essential for an effective response to threats and attacks.
- Technology increases security.

** Mineta IISTPS Report "Protecting Surface Transportation Systems and Patrons from Terrorist's Activities," 1997.*


Depth (Ft)
90'
60'
30'
0
-30'
Vent Shaft
Vent Shaft
Fan Shaft
Vent Shaft
P1
Vent Shaft
Fan Shaft
Vent Shaft
Vent Shaft
Fan Shaft
Vent Shaft
Vent Shaft
Scale
0
600
1,200
Feet
S
A Station
P2
B Station
P3
10 min
C Station
D Station
Legend
No Access Between Tracks
Station Platform
Fan Controls
OS&Y Ladder
Ladder Access
Stair Access
S Source
P Points of Interest
X Crossover Between Tracks

Three–hour exposure from subway venting from each source.



West Entrance

Fan Shaft

East Entrance

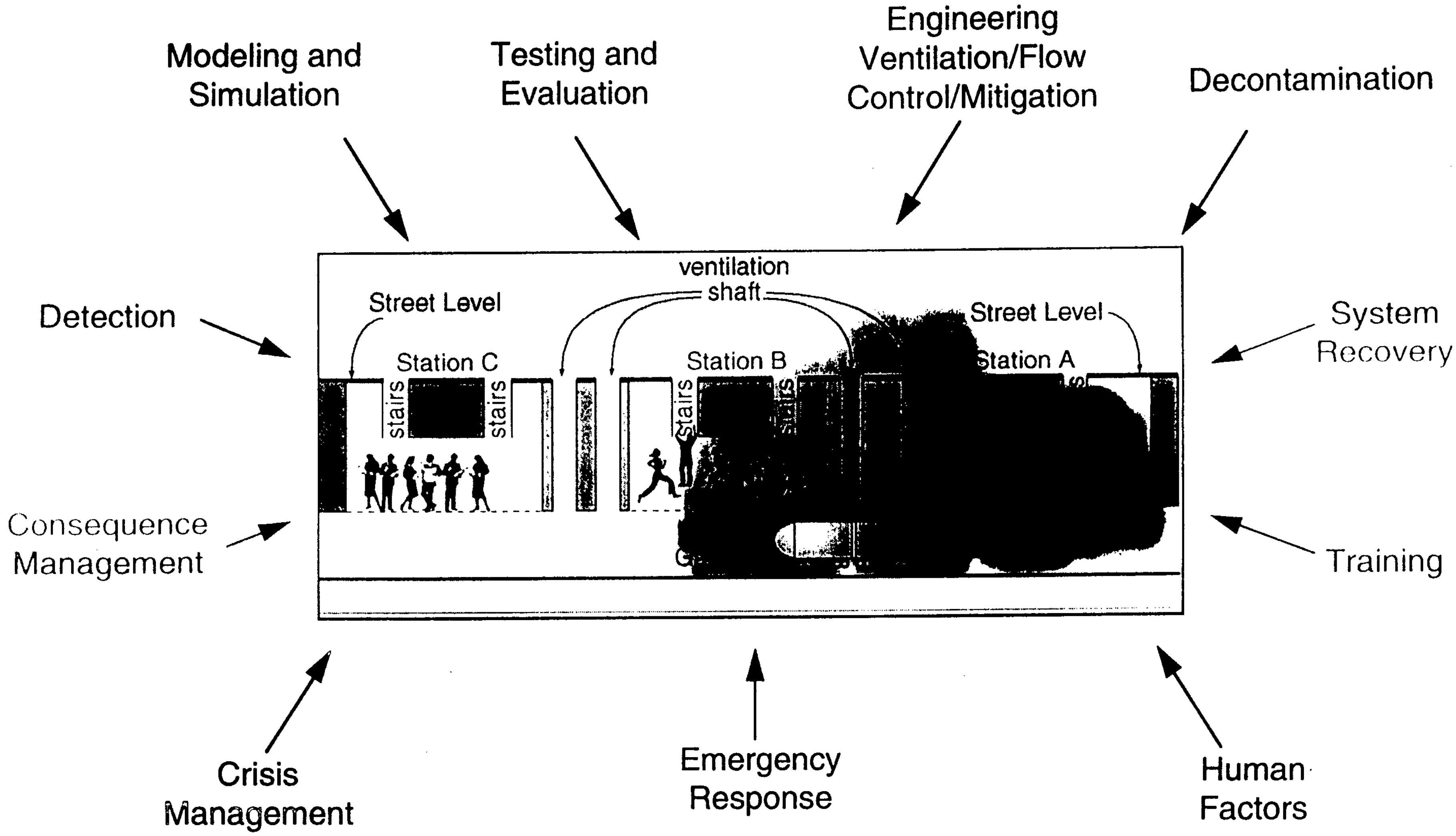
All Sources

Sample Subway System C/B Impacts

	Biological Agent Attack		Chemical Agent Attack	
	Fatalities	Exposed	Fatalities	Exposed
In-stations	7,400	53,500	240	1,200
On Trains	22,400	14,700	1,800	6,900
Above Ground	10,000	95,000	10	200
Total	40,000	163,000	2,000	8,500

Notes: Biological agent attack assumes no detection. Chemical agent attack assumes halting trains 15 minutes after attack.

Chemical/Biological Release in Subway System



Modeling and Simulation

Testing and Evaluation

Engineering Ventilation/Flow Control/Mitigation

Decontamination

Detection

System Recovery

Consequence Management

Training

Crisis Management

Emergency Response

Human Factors

PROTECTS Program Thrusts

Effects Modeling
- Develops effects and hazard modeling tools
- Performs subway system vulnerability and response assessments

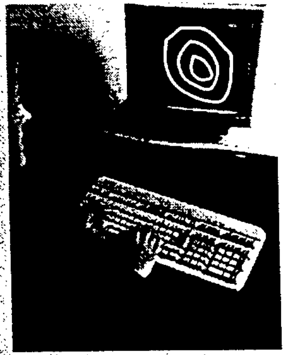
Engineered Responses
- Analyzes air flow control and in-station mitigation measures
- Demonstrates near-term station upgrades

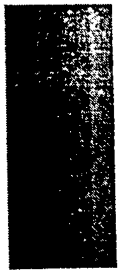
Warning and Control
- Assesses and demonstrates sensors (chem and bio)
- Addresses integration of sensors into operational controls

Training and Exercises
- Develops software tools for first response
- Assists in specification of realistic exercise plans

Integrated C/B Infrastructure Protection Program
Subway Pilot Project – Washington D.C. Metro

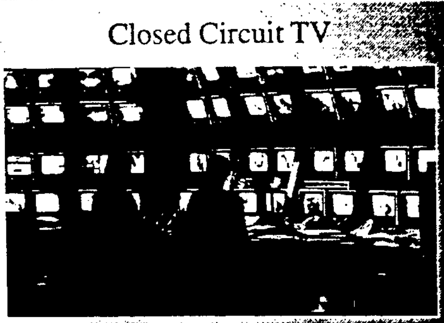
Modeling Above-Ground Below-Ground Impacts





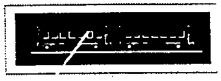
C/B Detection

Closed Circuit TV



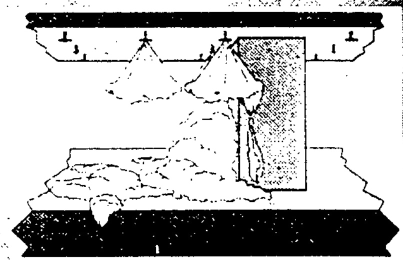
Training Too!s

- Simulator or virtual reality environment
- Visualization of C/B events



Operations Control Center (OCC) C/B Emergency Response Software

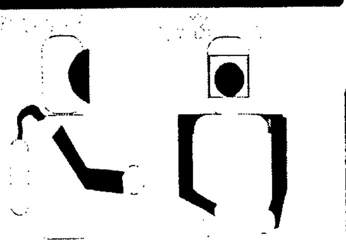
Equipment to Reduce Station Impacts (e.g. sprinklers, incinerattors)



First Responder Emergency Response Tools

- Portable PC
- Videotape of stations/tunnels
- C/B symptons, treatment
- Communications link to OCC

Equipment to Stop Tunnel Air Flow (e.g. inflatable barrier)



Decontamination

- Techniques for controls

Emergency Plans and Exercises

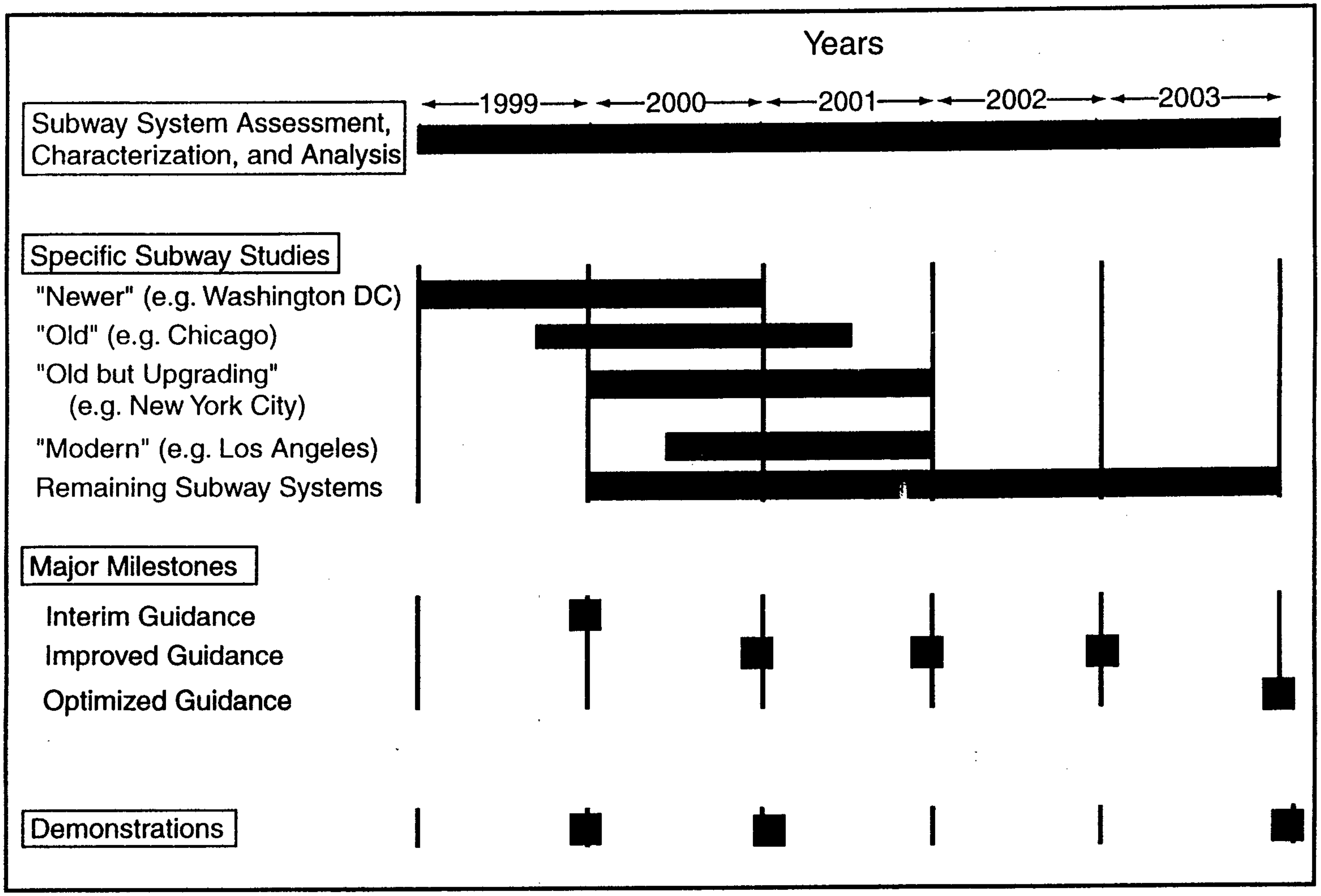
- C/B consequence management plans
- System-wide exercises

Infrastructure Protection Domestic Demonstration and Application Program

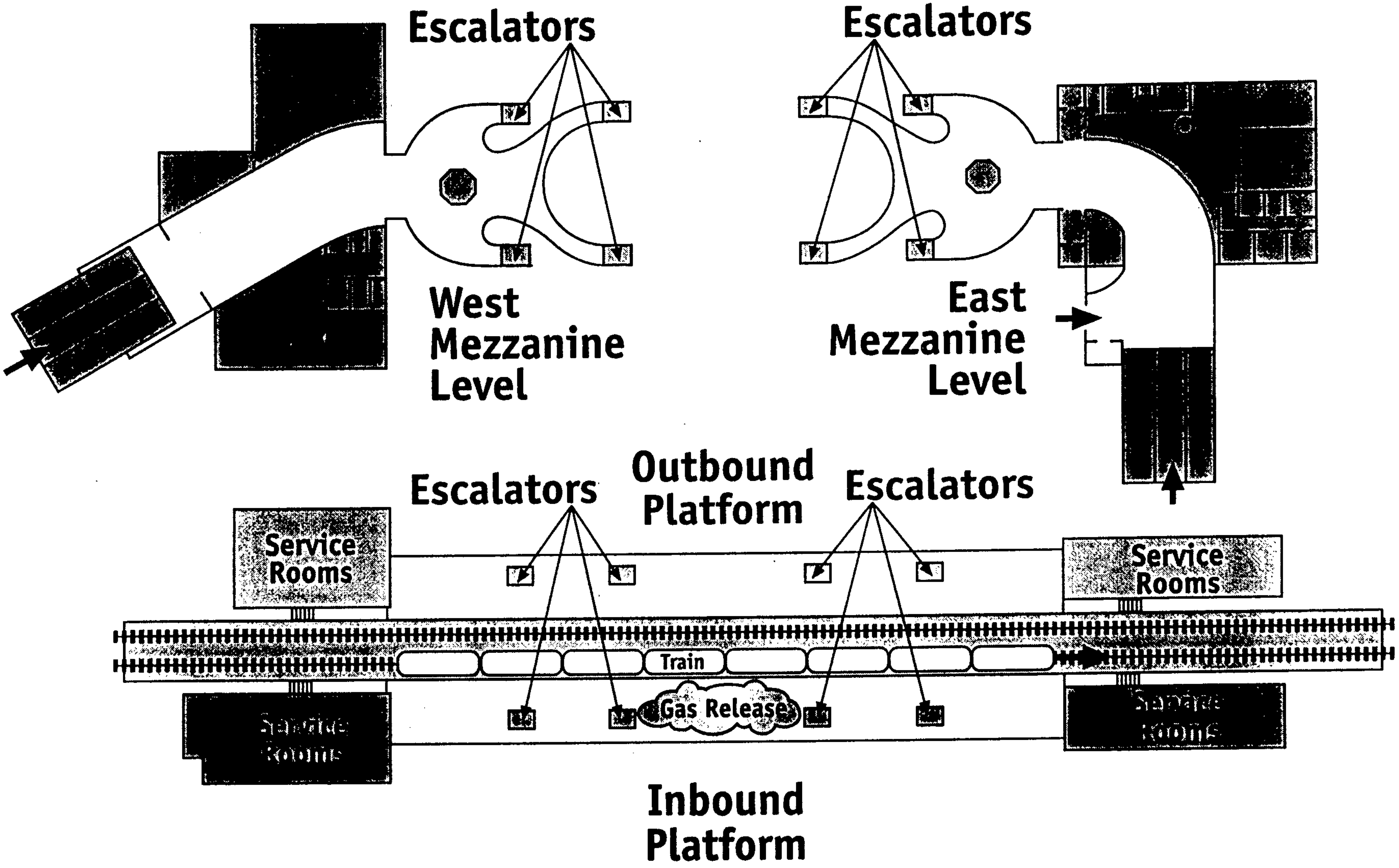
Objective: Field technologies and analysis tools to protect “at risk” facilities; pilot-study with Washington METRO

- Integrated sensor network at 5 subway stations
- Closed circuit TV
- Interior modeling and predictions codes linked to sensors
- Central control linkage with electronic response protocols
- Systemwide response with SOPs
- Response and Safety Plan upgrades
- Exercises (with tabletops, drills)

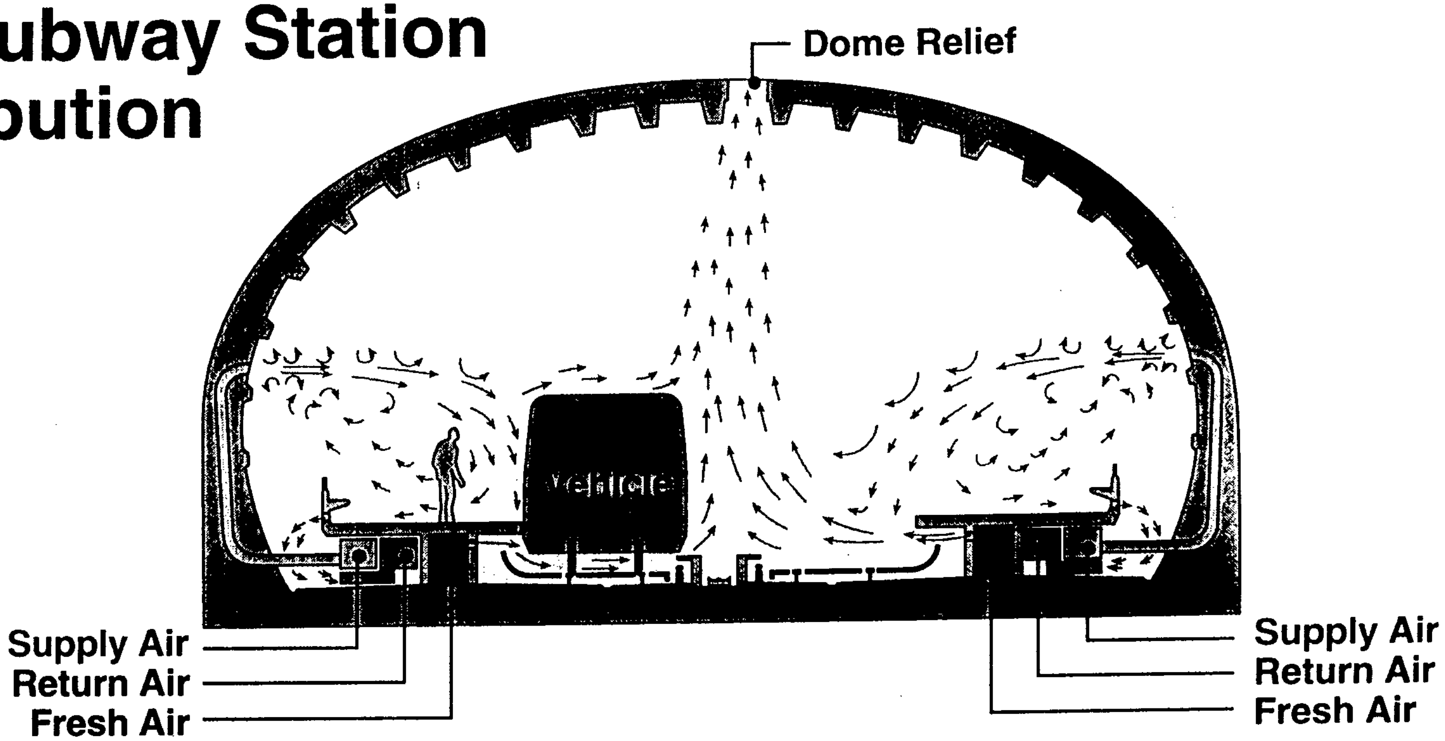
Time Schedule for Preparing U.S. Subway Systems for Chemical/Biological Terrorism



Typical Subway Station – Top View



Typical Subway Station Air Distribution



Poison Gas Scenario

Release on (Side) Platform

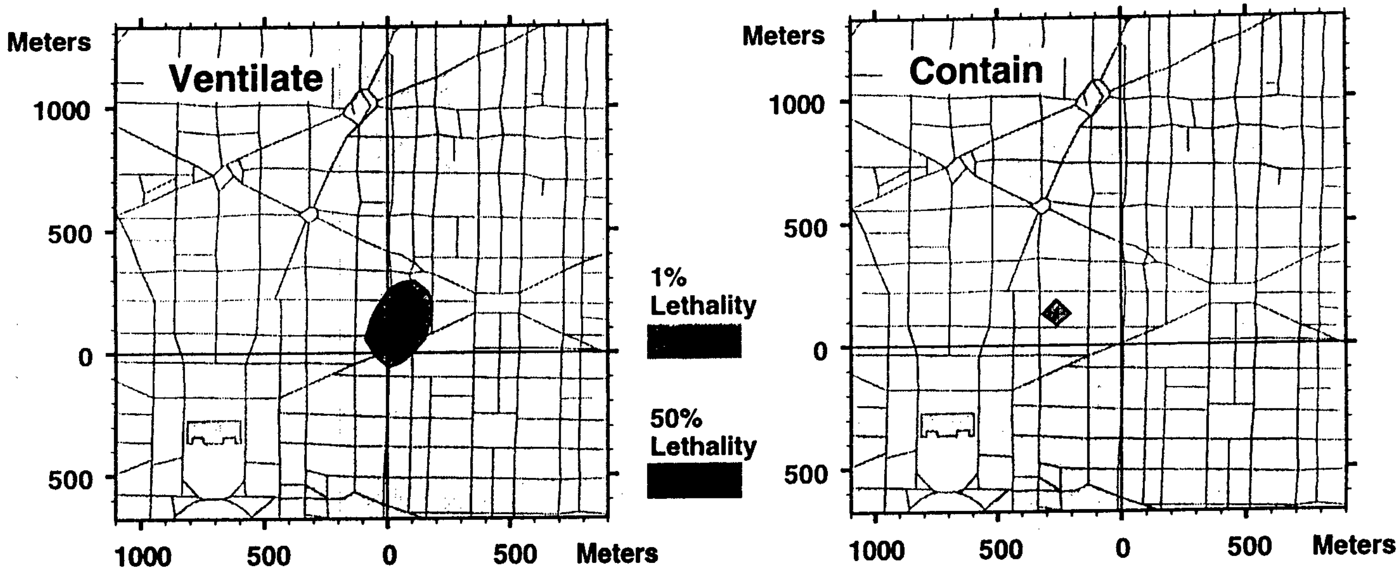
- Rush hour trains in opposite directions
- Emergency management 6 minutes after release
- Release in mid-platform with train in station)

Compare

A - Tunnel fans on, trains stop (ventilate)

B - Tunnel fans off, trains stop (contain)

Street Impacts



3 Hours from Release

	% Agent		% Agent Outside
	In Station	In Tunnel/ Vent Shafts	
Ventilate	< 1	< 1	99
Contain	75	3	21

Final Comments

- Subway systems are NOT prepared for C/B terrorism.
- Deterrence and prevention are difficult – more attention needed to mitigate casualties, damage, and rapidly restore service.
- Technology can enhance emergency management but needs integrated systems approach including field exercises and training.
- Security technology best included in original design and construction.

Final Comments (cont.)

- Most favored technology additions are multi-purpose and reduce security operations costs.
- Multi-mode communications are essential.
- Lessons learned need to be transferred to all subway systems.
- Advance planning is essential to effective response to threats and incidents.

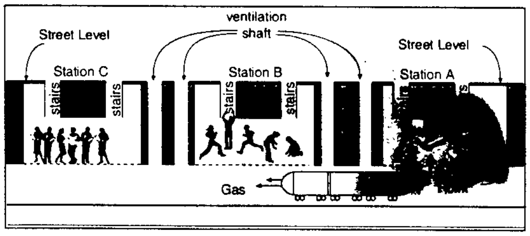
PROTECTS*

*Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism in Subways

Addressing a Critical Need

The March 1995 sarin attack in the Tokyo subway by a small group of extremists brought into sharp focus the vulnerability of U.S. subway systems to a similar chemical or biological (C/B) attack. The underground tunnel network of a subway system, with its moving trains and many ventilation shafts to the surface, can distribute a C/B agent throughout many stations and tunnels below ground and through ventilation shafts above ground to an entire city (see Fig. 1). Recent studies show that an incident involving anthrax can expose more than 100,000 people with an associated cost of more than 26 billion dollars.

The Threat: Chemical/Biological Release in Subway System



- Terrorist releases poison gas in Station A
- Movement of train spreads gas to Station B
- Gas can escape to street level and poison people there too

Figure 1. Sketch of Chemical Agent Release in Subway

Emergency-response exercises carried out after the Tokyo incident in New York City, Boston, and Washington, D.C., have revealed a critical need for improved planning and emergency response procedures to save lives in the event of a C/B attack.

The knowledge needed by first responders as well as those involved throughout the subway system is lacking, as are the personal protection equipment and detection equipment needed to handle such an event. A modest investment in technology and advanced planning now can yield enormous benefits in the future.

Transit authorities need an *integrated* approach that covers preplanning for such incidents as well as emergency response during an event. PROTECTS is such a program, since it will develop new technology (hardware and software) and emergency planning recommendations before incidents occur and advanced emergency manage-ment tools for incident response. PROTECTS will provide this technical assistance and a practical approach for implementation to all U.S. subway systems.

A Cooperative Federal, State, and Local Program

The proposed program is envisioned as a cooperative effort among transit authorities, federal/state/local emergency response organizations, and government officials. Final products of this work cover the broad areas of engineering solutions to limit human and system impacts; tools and recommendations for emergency response and training; and methods for decontamination and recovery. Owing to the comprehensive nature of the program, PROTECTS will potentially include all key federal organizations with an active interest in this area, including the U.S. Department of Energy (DOE), Federal Transit Authority (FTA), U.S. Department of Defense (DOD), and Federal Emergency Management Agency (FEMA). The involvement of user groups at each stage of the program will ensure that the final products match the capabilities and requirements of the potential users. A close working relationship among project personnel, emergency response organizations, and transit authorities is essential to the success of the program.

PROTECTS is envisioned as a conceptual plan to prepare U.S. subway systems to better respond to C/B incidents. It is expected that PROTECTS would be administered by a multi-agency group.

Leveraging Ongoing Programs

PROTECTS is a natural outgrowth of ongoing programs sponsored by DOE, DOD, FTA, the U.S. Department of Transportation (DOT), FEMA, and existing transit authorities for responding to potential terrorist attacks and fires. In the area of modeling and simulation, DOT has supported years of development of the SES (Subway Environment Simulation) model that predicts air flow rates and cooling loads within a subway system as a function of time. Inflatable barrier studies such as those conducted by the Washington METRO (WMATA) provide a good point of departure for further work on containment strategies. The Technical Support Working Group (TSWG) of the Office of the Secretary of Defense is supporting an evaluation of the current generation of chemical sensors for possible use in subway stations. DOD and DOE have supported numerous long-term efforts related to C/B agent sensors, decontamination, dispersion modeling, and emergency response planning. PROTECTS builds on the successes of these past and current federal agency programs.

Elements of PROTECTS

Figure 2 shows the seven major elements of PROTECTS.

1. Modeling and Simulation

This element will identify the consequences of a range of scenarios that deal with releases in stations, train cars, and ventilation shafts. Predictions of transport and fate for this wide variety of scenarios will be used to identify the best mitigation and consequence management strategies in case of a terrorist incident. Modeling will also be used to study the effect of containment barriers and to define the proper operation and settings of ventilation fans to minimize the impacts on people both in the subway and above ground. The Washington METRO will serve as the initial study site; additional subway systems will be added as the study progresses so the effect of different subway system designs on the results will be fully considered.

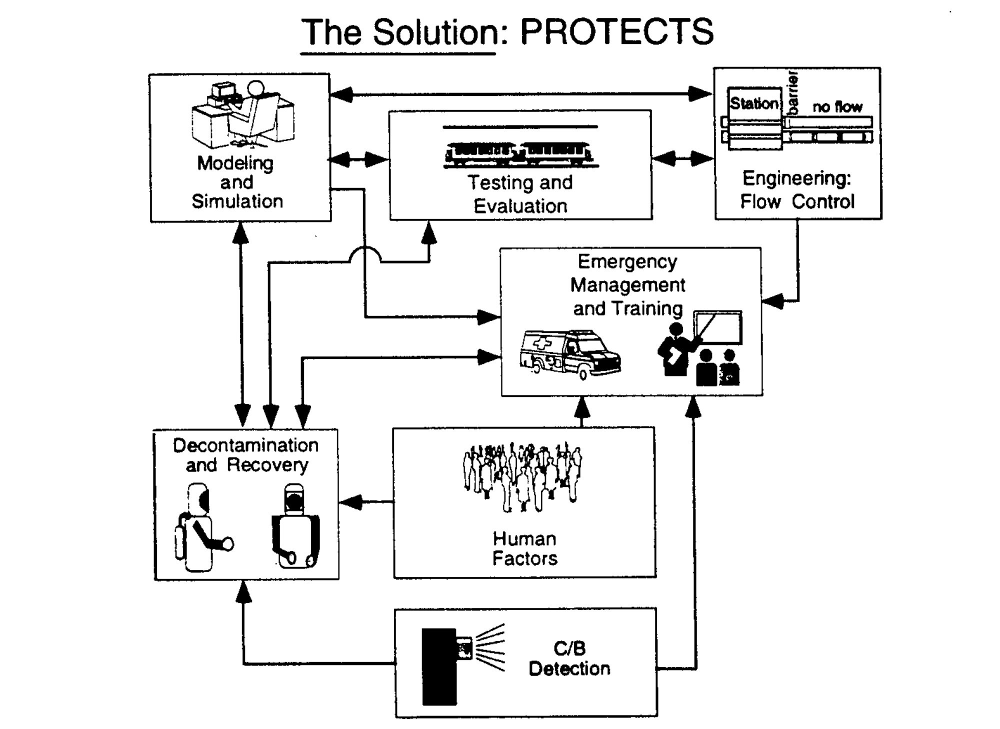


Figure 2. The Seven Elements of PROTECTS

2. Engineering – Flow Control

Mitigation options will be greatly enhanced if independent control of tunnel and station air flow patterns can be achieved. Allowing a C/B agent to spread unchecked throughout the entire subway system and ultimately to the surface can potentially expose large numbers of people. Ventilation control can be used to either confine the C/B agent plume to a particular section of tunnel or alternatively to disperse the plume as rapidly as possible. Much is known about ventilation techniques; much less is understood concerning flow control. The best option for a specific incident will depend on the location and nature of the release. Controlled ventilation can also be used to clear escape routes for passengers and access routes for emergency response personnel. Correct control modeling of ventilation flow within the subway system is the critical element in developing the most effective strategy for a particular event. This element evaluates and develops new methods for flow control in support of modeling recommendations mainly using new design and experimental techniques.

3. Testing and Evaluation

Because the results from both elements above may ultimately form the basis for significant upgrades to existing systems, both the accuracy of the analysis and the efficacy of the flow control system will need to be validated by field testing. Such tests will have to be conducted so as to have only a minimal impact on transit system operation. All dispersion testing will be done by using harmless simulants subject to authorization by the respective transit authority. The testing of decontamination methods with subway materials will be done in the laboratory.

4. Detection of Chemical and Biological Agents

Although work on new sensor technologies is progressing at a steady pace, electronic sensors of C/B agents are at an early stage of development and thus cannot be relied on at present for automated event detection. Despite this state of affairs, portable and fixed C/B sensors can be used to confirm an incident, identify the specific nature of the agent or agents being used, support mitigation actions, and aid in rescue operations. The combination of C/B sensors and real-time computer simulations can be a powerful tool for crisis management. A long-term program for protecting the nation's subway systems must include the ongoing consideration and evaluation of sensor options and factor in new sensor technologies as they become available. Until sensors are available and reliable, human observation and intelligence information will be used to identify an incident.

5. Human Factors

The human factors element of the proposed program involves determining how to best manage people and enable them to most efficiently communicate information during an emergency. Issues of concern include (a) how to best manage rider behavior, (b) how transit workers can best identify and report an incident most efficiently, (c) how to collect incident information and evidence in the most usable form for forensic and scientific evaluation, and (d) how riders can become alert observers for the transit authority without becoming alarmed. A related issue is how passengers can learn to take part in their own rescue.

6. Emergency Management and Training

This element involves the implementation of strategies developed from elements 1 through 5 above and includes (a) development of first responder procedures, (b) development of Operations Control Center protocols, and (c) coordination of rescue operations with city, state, and federal response organizations.

To aid transit authorities and response organizations in preparing emergency plans, a manual that examines all issues relevant to C/B incidents will be developed. The manual will address initial incident identification through crisis management and ultimately postevent activities. Team scientists will partner with transit authorities and federal, state, and local agencies to assist them in developing appropriate emergency response protocols. In addition, responders will provide feedback to the team scientists to ensure that the manual meets their needs.

Technological solutions are only as good as the training provided on how to use them. Past fires in subway systems have revealed that inadequate training is the biggest impediment to proper emergency action. Poor emergency management outcomes are also caused by human error and the gap between high-technology solutions and the capability of transit workers to use them. Although technological solutions have often worked well, the inability of transit workers to effectively use the technologies has been problematic. The integration of response options and technological solutions into transit system operations involves the training of and exercises by (a) subway workers; (b) emergency response workers; (c) Operations and Control Center staff; (d) local, state, and federal agencies; and (e) public affairs and media personnel. Drills must take place regularly to refresh, reinforce, and update trainees on key concepts. Training materials and classes on the tools developed specifically for this program will be prepared. A team of technical staff will also provide broader guidance through workshops and reviews of in-house training programs, as needed.

Finally, a computer program will be developed as a training tool to show trainees how C/B agents disperse in [illegible] and inform them about the outcomes of specific emergency response options.

7. Decontamination and Recovery

Studies will be carried out to evaluate the most effective methods for decontaminating subway tunnels and stations. Both agents contained in the air and agents deposited on surfaces will be considered. Procedures and equipment for such work will be identified for transit authority consideration. Laboratory studies will determine if the proposed methods will be sufficient for ensuring passenger safety on the basis of their proposed frequency and intensity of application. A protocol for sampling after cleanup is also needed to assure that decontamination has been successful and that it is safe for passengers to re-enter the subway. If available methods for decontamination are found to be inadequate, new approaches will be developed. This effort will be updated periodically to incorporate scientific advancements.

Two-Track Effort for Subway Systems

U.S. subway systems vary in terms of their (a) technology (old to modern systems), (b) mix of underground and aboveground sections, and (c) tunnel construction techniques. Most systems need to upgrade their emergency ventilation capabilities to meet current standards for fire and smoke incidents. This requirement provides an impetus for subway systems to research ways to meet both fire/smoke and C/B challenges by using compatible, cost-effective methods. Such methods do exist.

The U.S. subway systems can be placed into four categories on the basis of the character of their ventilation systems and their likely need for different C/B solutions:

(1) "modern" (e.g., Atlanta, Los Angeles, Buffalo)

(2) "newer" (e.g., Washington, D.C., San Francisco)

(3) "old but upgrading" (e.g., Boston, parts of NYC), and

(4) "old" (e.g., Chicago, Philadelphia, Newark, parts of NYC).

A representative system from each of these categories will be studied to determine general principles for preplanning, mitigation, and emergency response.

WMATA, the Washington METRO, is

identified for a fast-track effort since it is the most vulnerable target politically and has been at the forefront of both fire/smoke mitigation and C/B protection efforts. Such efforts have focused on inflatable barriers for fire/smoke applications, and that flow control option is being considered again for both fire/smoke and C/B protection.

Three-Phase Program and End Products

The PROTECTS program schedule (Figure 3) shows the time each of the four characteristic subway systems will be studied. In addition, a general study of subway systems assessment, characterization, and analysis will be conducted starting in the first year; it will include all elements and subway systems. This work will identify general trends and principles as quickly as possible to allow development of emergency response plans on the basis of the best scientific information available at that time. That general task will continue in Years 2-5.

Phase I (Year 1) work will concentrate on providing interim guidance for each element for each of the four subway system categories on the basis of available information and modeling work done in that first year. Phase II (Year 2) will enhance the guidance of Phase I on the basis of what can be done in Year 2. Any technological breakthroughs in Years 1 and 2 will be incorporated

Once the approach to the seven elements is defined for any of the four prototypes, technologies will be immediately transferred to similar systems in the same category. However, some refinements will probably be required to account for site-specific details of design and operation.

as they occur. Phase III work (Years 3-5) will represent progress for all elements and subway systems (incremental to Phase II) for which technology improvements are needed in most elemental areas. The PROTECTS program will provide more advanced recommendations in each of the seven elements at the end of each of the five years for all subway systems.

To apply the technologies and lessons learned to all subway systems at the earliest time, three demonstrations are planned. At the end of both Year 1 and Year 2, a demonstration of the operation of the advanced technology and emergency response capability for one subway system will be presented. At the end of Year 5, a similar demonstration for a different system is planned.

The major end products of this program will be:

1. Technical tools for planning and developing emergency response strat-

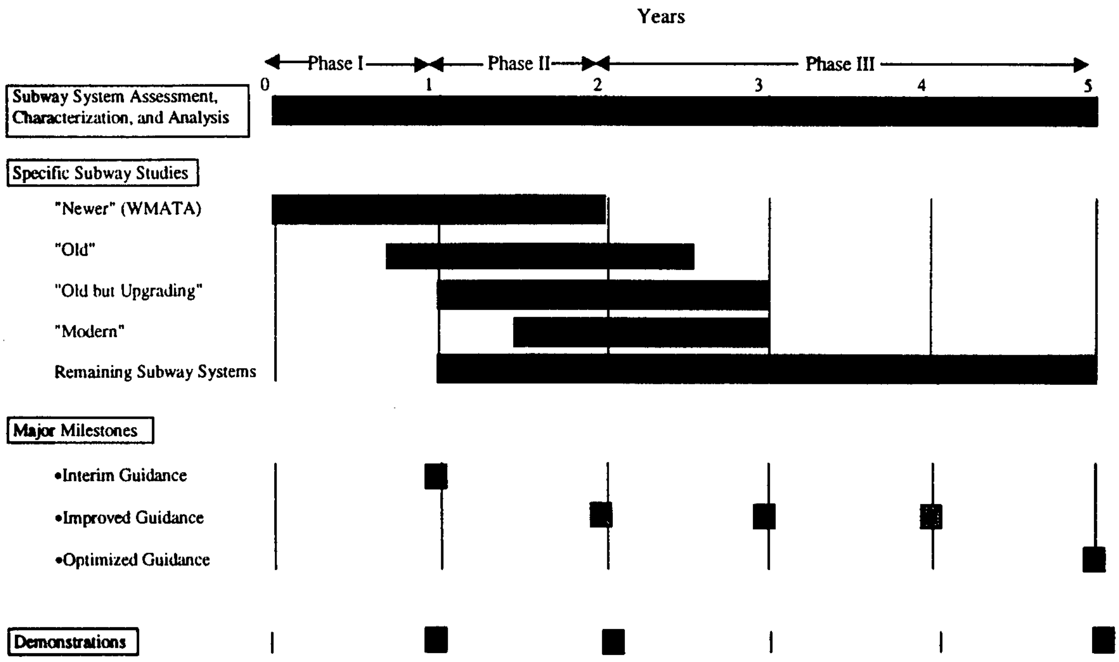
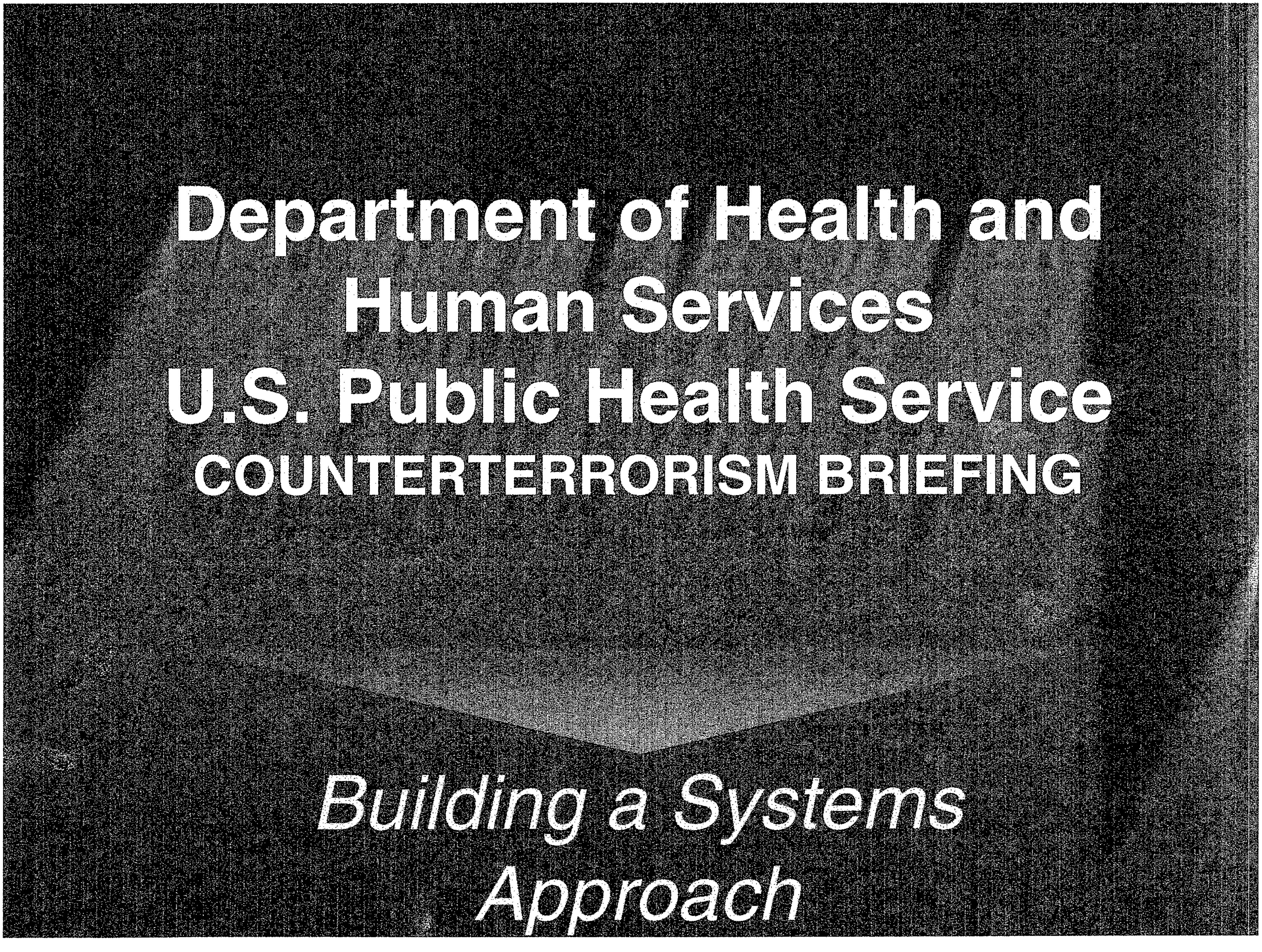


Figure 3. Conceptual Work Plan and Time Schedule for PROTECTS

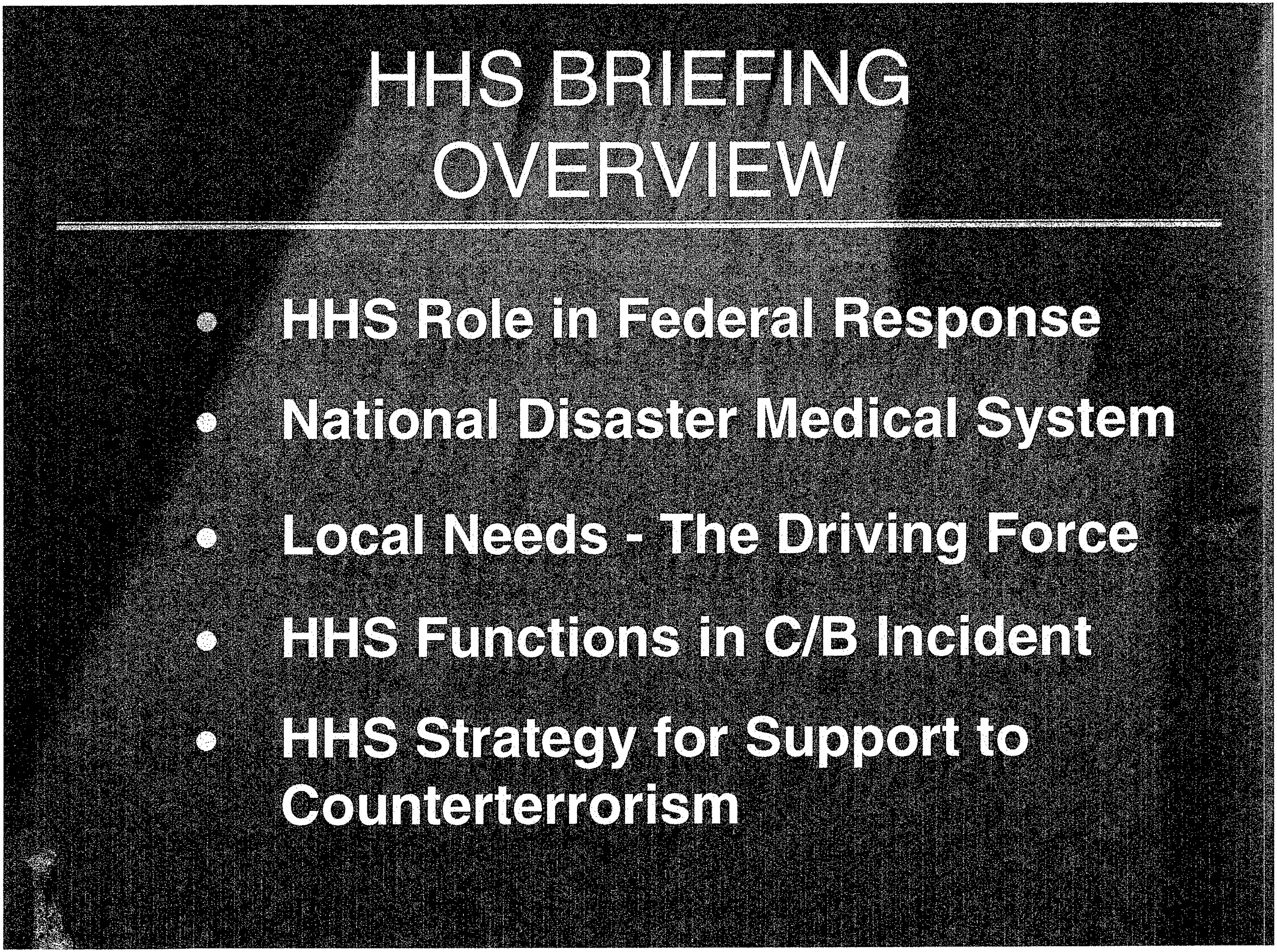
egies,

2. Recommendations of engineering solutions that will limit adverse impacts and protect both emergency responders and the general public,
3. Manuals for developing emergency procedures that will mitigate consequences and thus save lives during and immediately following an incident,
4. Technical assistance in implementing the program through training and exercises, and
5. Determination of methods and procedures for subway decontamination, recovery, and disruption minimization.



Department of Health and Human Services
U.S. Public Health Service
COUNTERTERRORISM BRIEFING

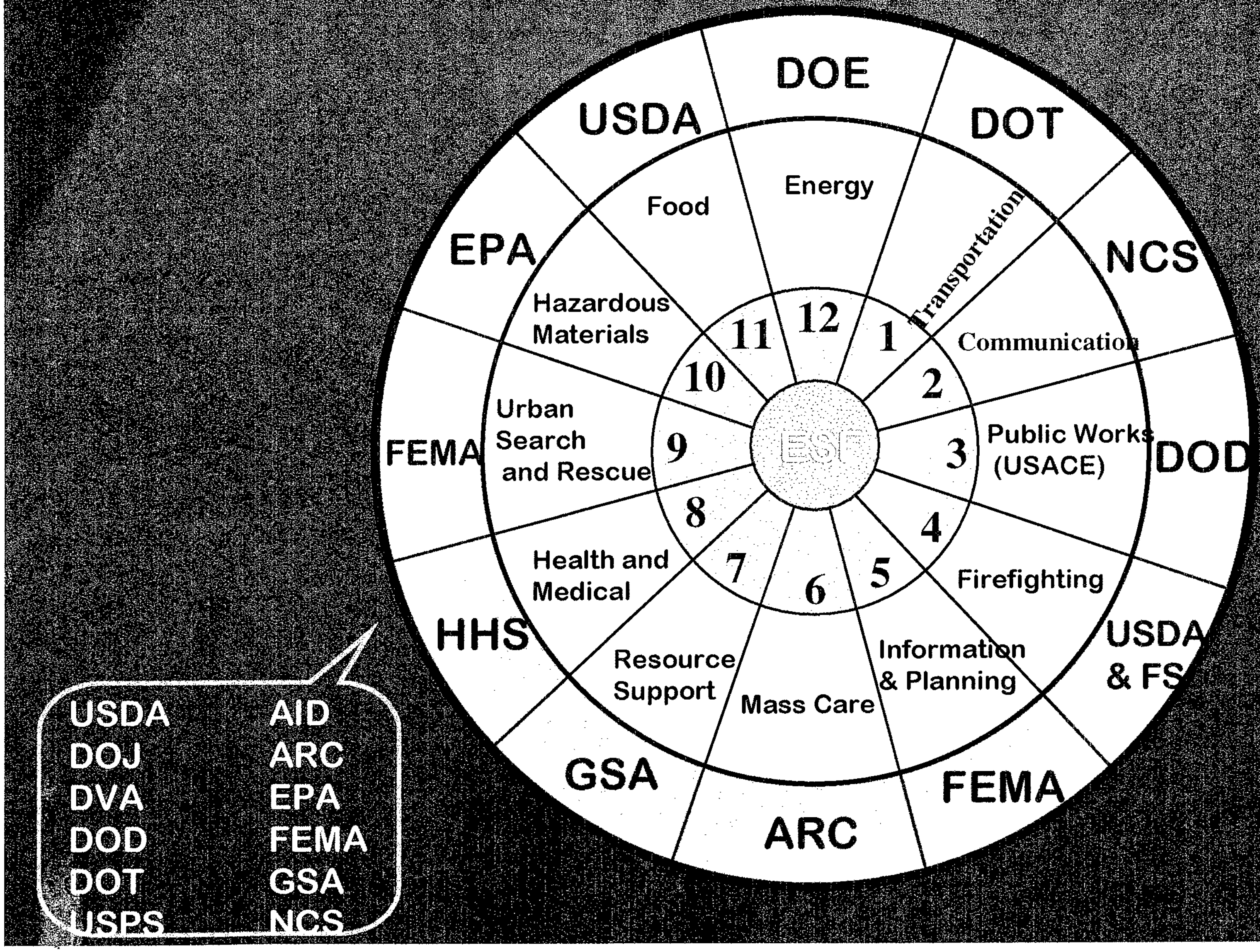
Building a Systems Approach



HHS BRIEFING OVERVIEW

- HHS Role in Federal Response
- National Disaster Medical System
- Local Needs - The Driving Force
- HHS Functions in C/B Incident
- HHS Strategy for Support to Counterterrorism

FEDERAL RESPONSE PLAN
EMERGENCY SUPPORT FUNCTIONS



ESF

1 Transportation DOT

2 Communication NCS

3 Public Works (USACE) DOD

4 Firefighting USDA & FS

5 Information & Planning FEMA

6 Mass Care ARC

7 Resource Support GSA

8 Health and Medical HHS

9 Urban Search and Rescue FEMA

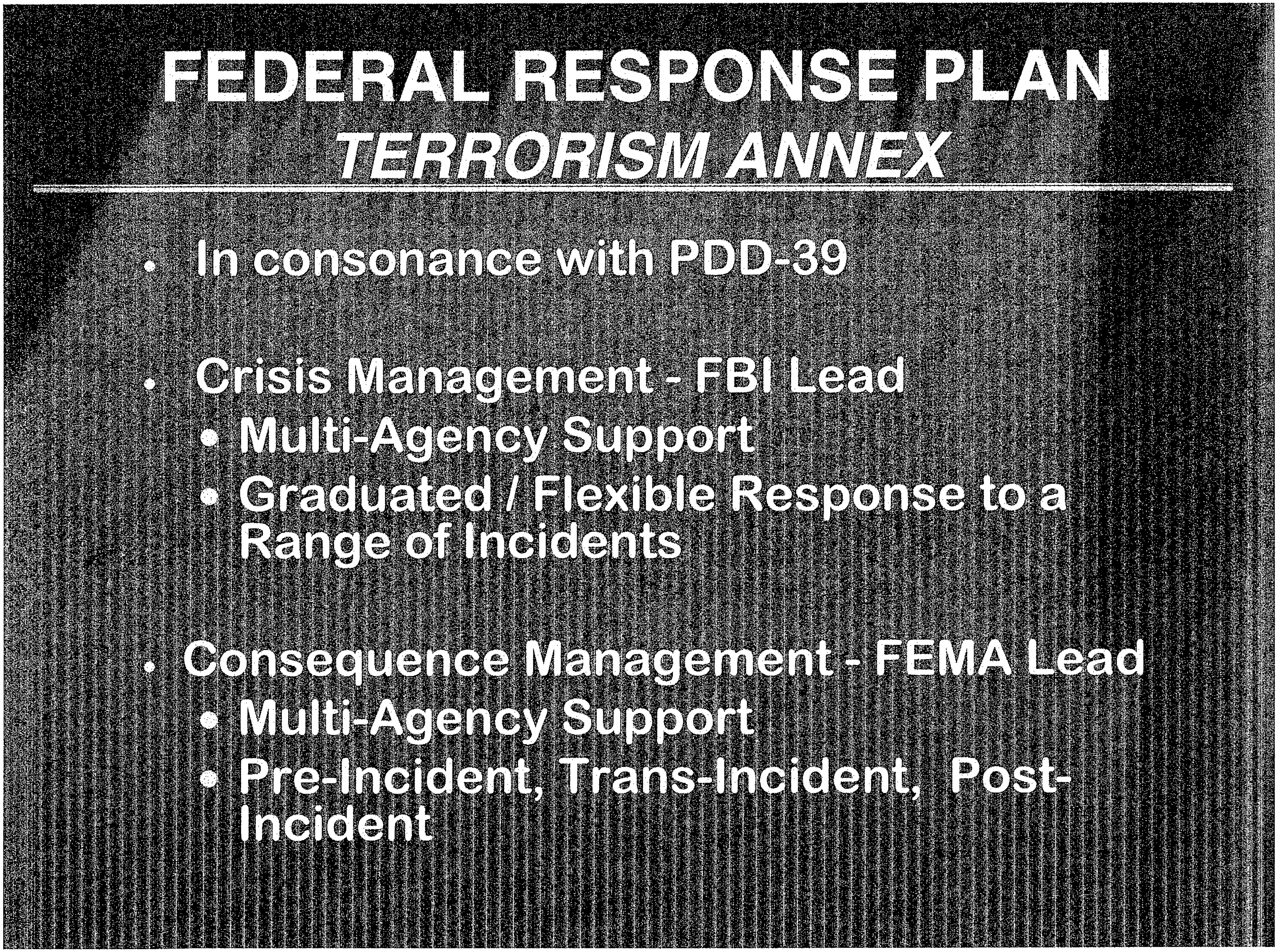
10 Hazardous Materials EPA

11 Food USDA

12 Energy DOE

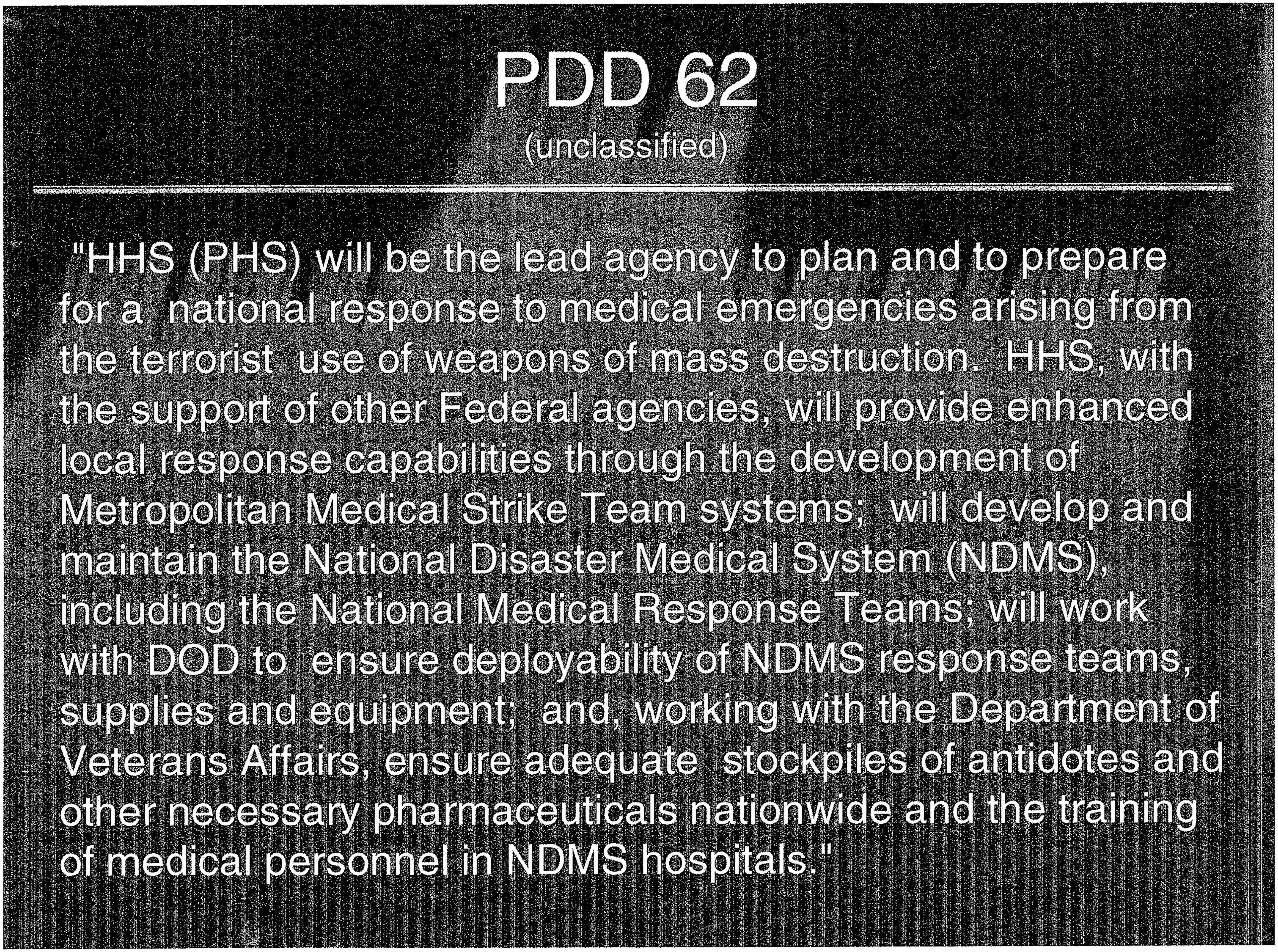
USDA
DOJ
DVA
DOD
DOT
USPS

AID
ARC
EPA
FEMA
GSA
NCS



FEDERAL RESPONSE PLAN
TERRORISM ANNEX

- In consonance with PDD-39
- Crisis Management - FBI Lead
  - Multi-Agency Support
  - Graduated / Flexible Response to a Range of Incidents
- Consequence Management - FEMA Lead
  - Multi-Agency Support
  - Pre-Incident, Trans-Incident, Post-Incident

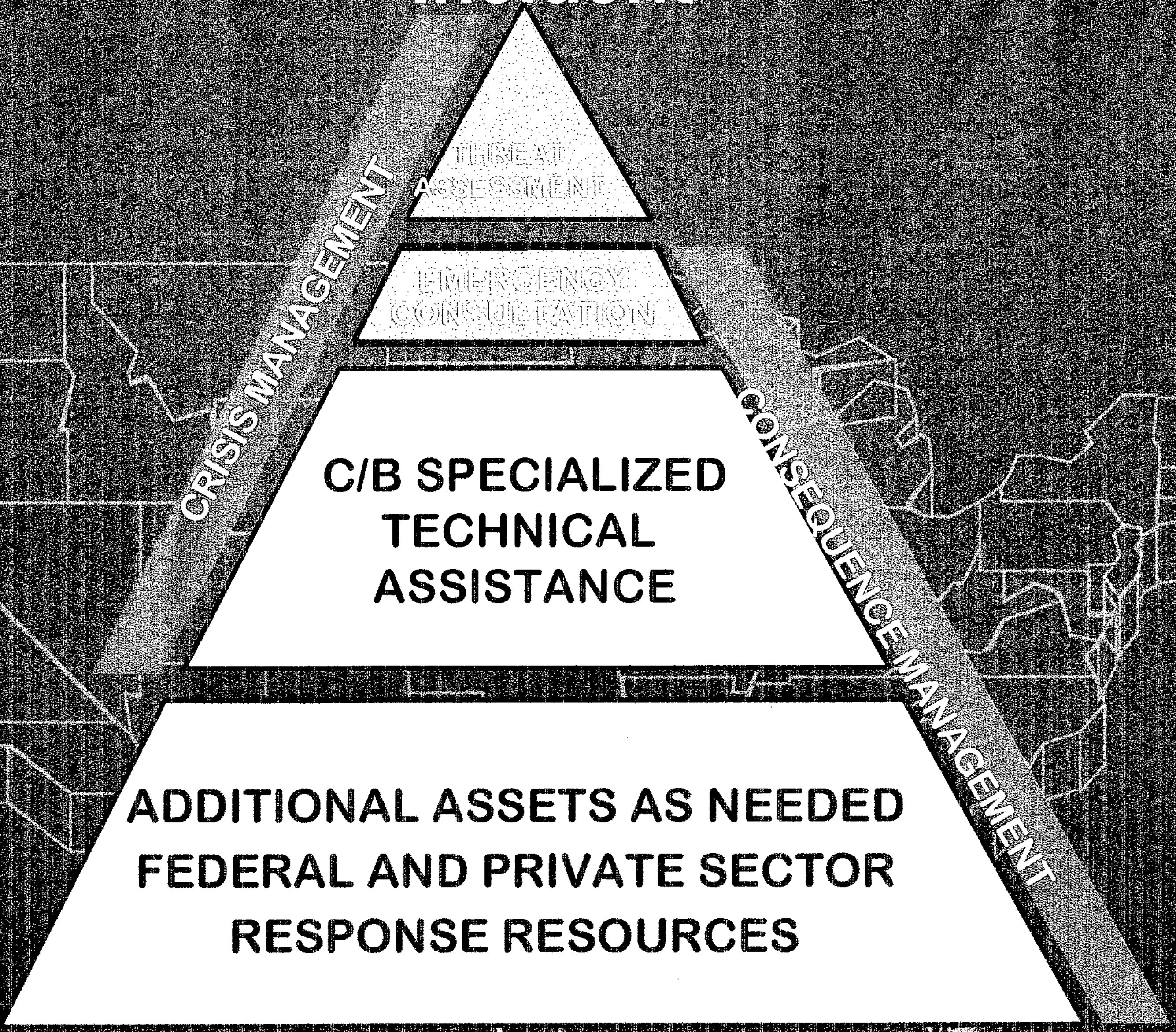


PDD 62

(unclassified)

"HHS (PHS) will be the lead agency to plan and to prepare for a national response to medical emergencies arising from the terrorist use of weapons of mass destruction. HHS, with the support of other Federal agencies, will provide enhanced local response capabilities through the development of Metropolitan Medical Strike Team systems; will develop and maintain the National Disaster Medical System (NDMS), including the National Medical Response Teams; will work with DOD to ensure deployability of NDMS response teams, supplies and equipment; and, working with the Department of Veterans Affairs, ensure adequate stockpiles of antidotes and other necessary pharmaceuticals nationwide and the training of medical personnel in NDMS hospitals."

Major Components for Response to C/ B Incident



THREAT ASSESSMENT

EMERGENCY CONSULTATION

C/B SPECIALIZED TECHNICAL ASSISTANCE

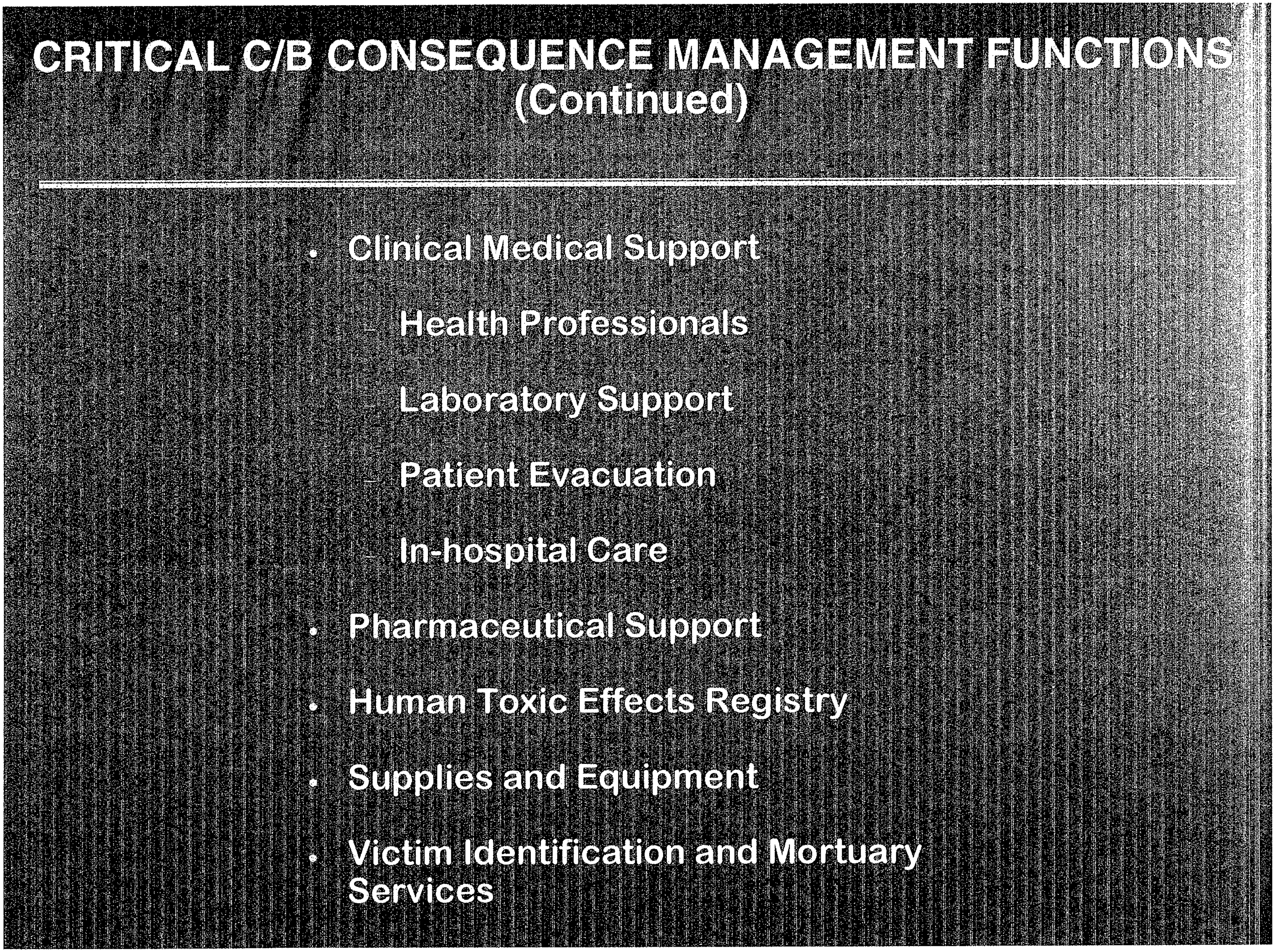
ADDITIONAL ASSETS AS NEEDED FEDERAL AND PRIVATE SECTOR RESPONSE RESOURCES

CRISIS MANAGEMENT

CONSEQUENCE MANAGEMENT

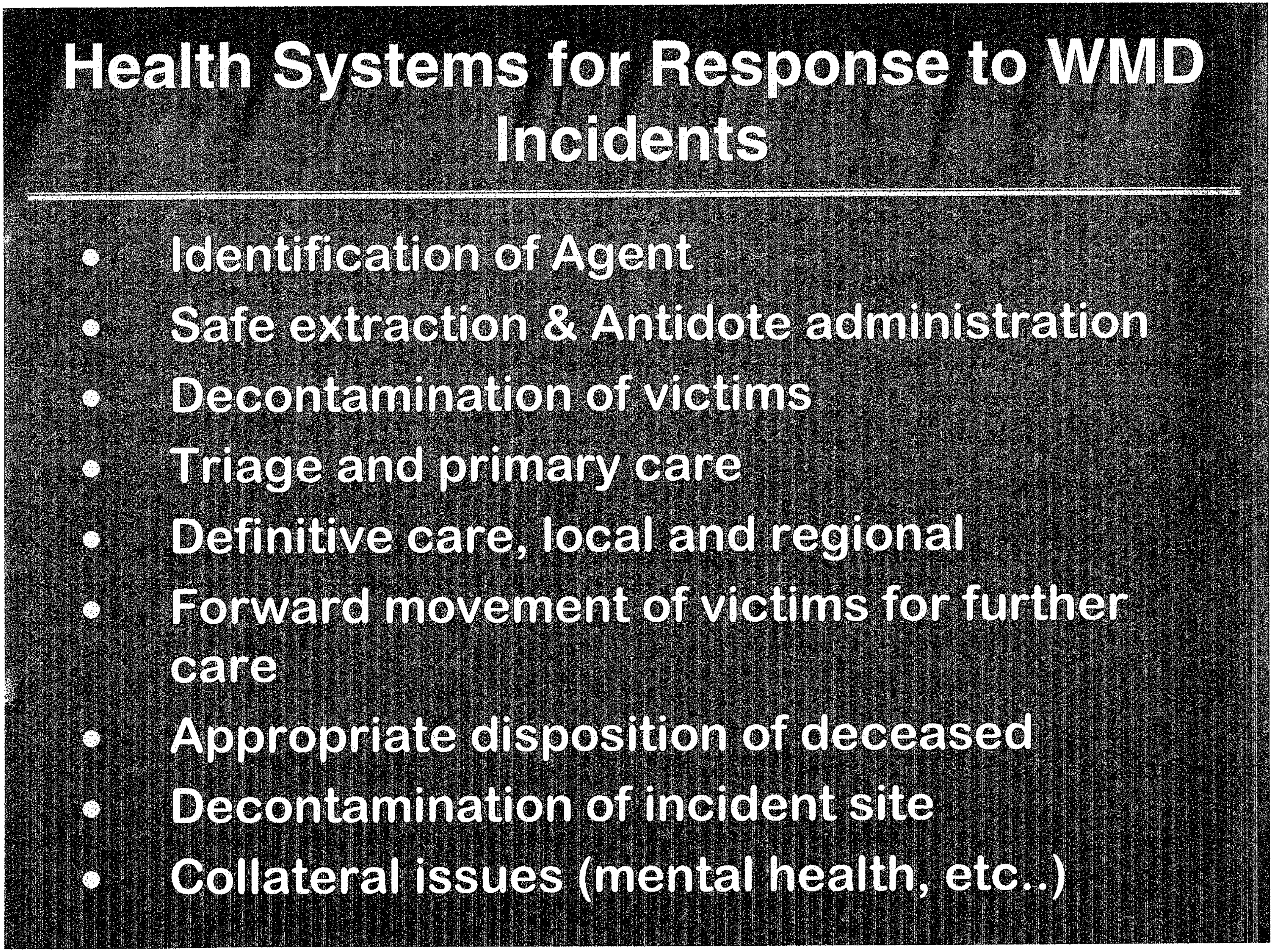
CRITICAL C/B CONSEQUENCE MANAGEMENT FUNCTIONS

- Threat Assessment
- C/B Consultation with Affected Jurisdictions
- Public Affairs
- Agent Identification
- Epidemiological Investigation
- Expedient Hazard Detection
- Expedient Hazard Reduction
- Environmental Decontamination
- Mental Health Support



CRITICAL C/B CONSEQUENCE MANAGEMENT FUNCTIONS (Continued)

- Clinical Medical Support
  - Health Professionals
  - Laboratory Support
  - Patient Evacuation
  - In-hospital Care
- Pharmaceutical Support
- Human Toxic Effects Registry
- Supplies and Equipment
- Victim Identification and Mortuary Services



Health Systems for Response to WMD Incidents

- Identification of Agent
- Safe extraction & Antidote administration
- Decontamination of victims
- Triage and primary care
- Definitive care, local and regional
- Forward movement of victims for further care
- Appropriate disposition of deceased
- Decontamination of incident site
- Collateral issues (mental health, etc..)

Local Health and Medical Needs

Most local emergency systems need enhanced capability to manage the threat or use of WMD

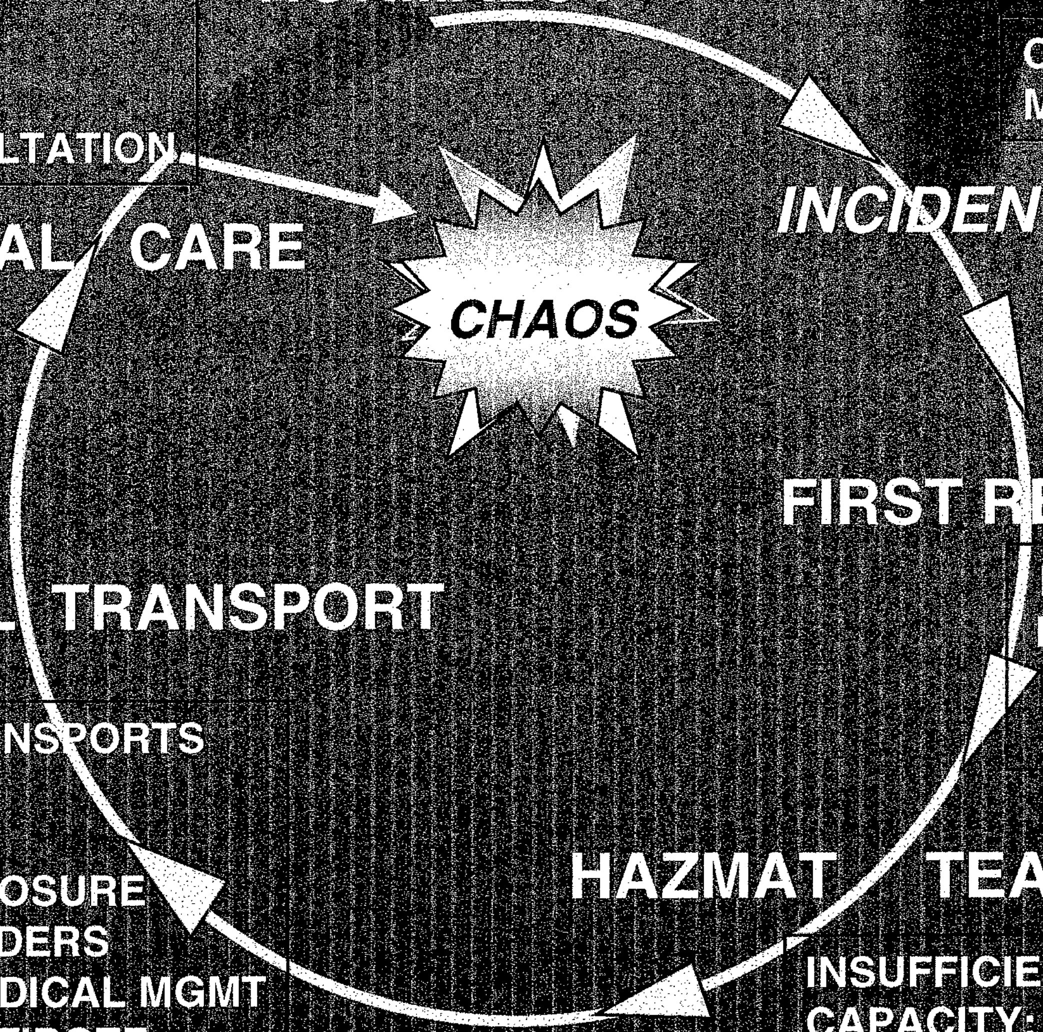
Major issues include:

- Agent Identification
- Most appropriate protection
- Decontamination (victims and environment)
- Treatment modalities
  - Initial
  - Definitive
- Diverse collateral requirements (public safety, mental health, etc...)

Tokyo Poison Gas Attack

- Emergency services unprepared
- No detection capability
- No on-scene decontamination
- No initial treatment
- 10% of first responder became victims from off-gassing
- Hospital admitted casualties with no regard to contamination
- Treatment initiated 2-3 hours post-exposure based on suggestions from physicians in Matsumoto
- Fortunate that it was a low lethality sarin concentration

INCIDENT LIFE CYCLE
WITHOUT PREPAREDNESS



NORMALCY

INCIDENT

FIRST RESPONDERS

HAZMAT TEAM

MEDICAL TRANSPORT

HOSPITAL CARE

CHAOS

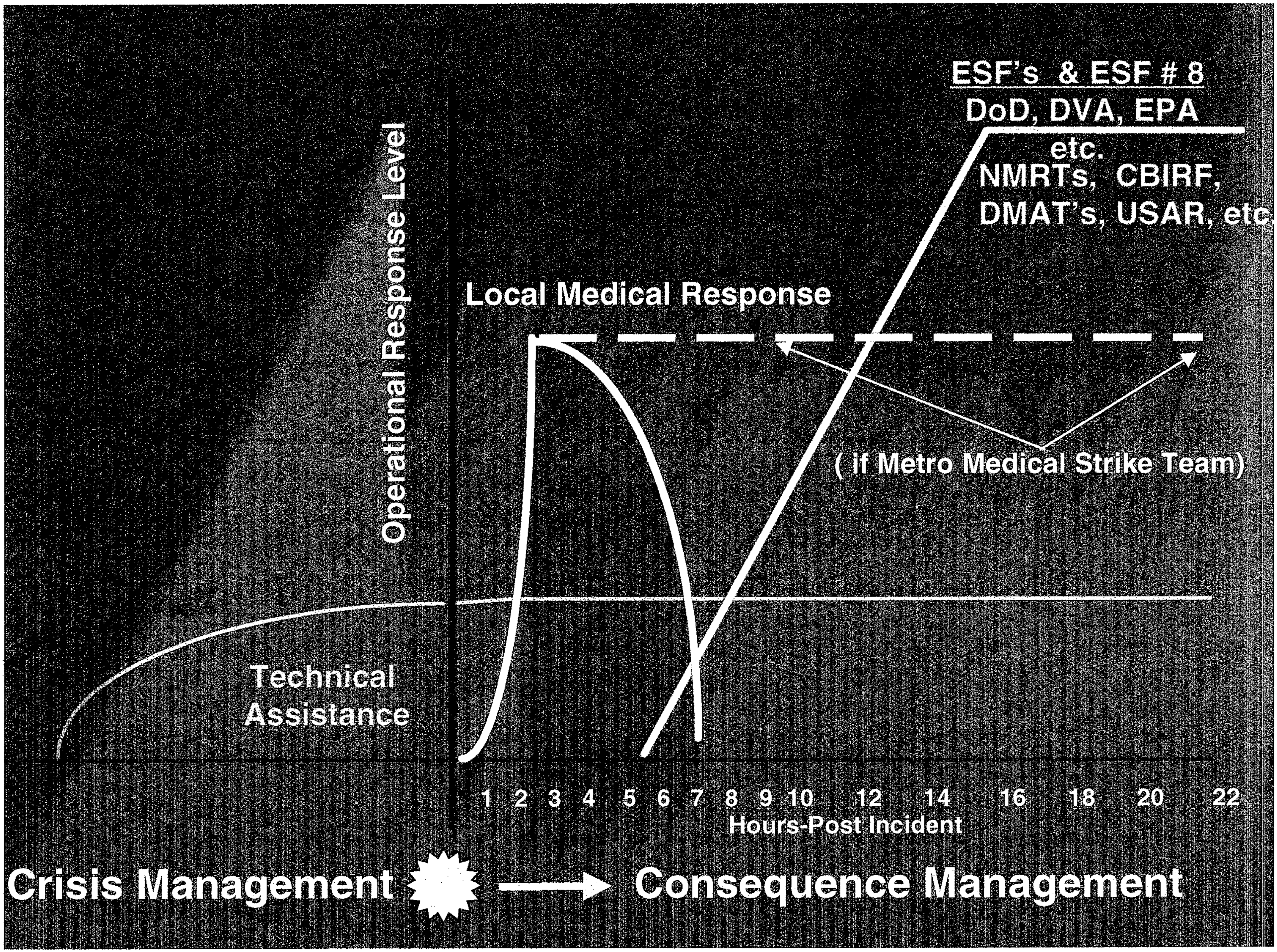
CONTAMINATED
MASS CASUALTIES

POLICE / FIRE / EMS
HAZARD EXPOSURE
INADEQUATE FIRST AID

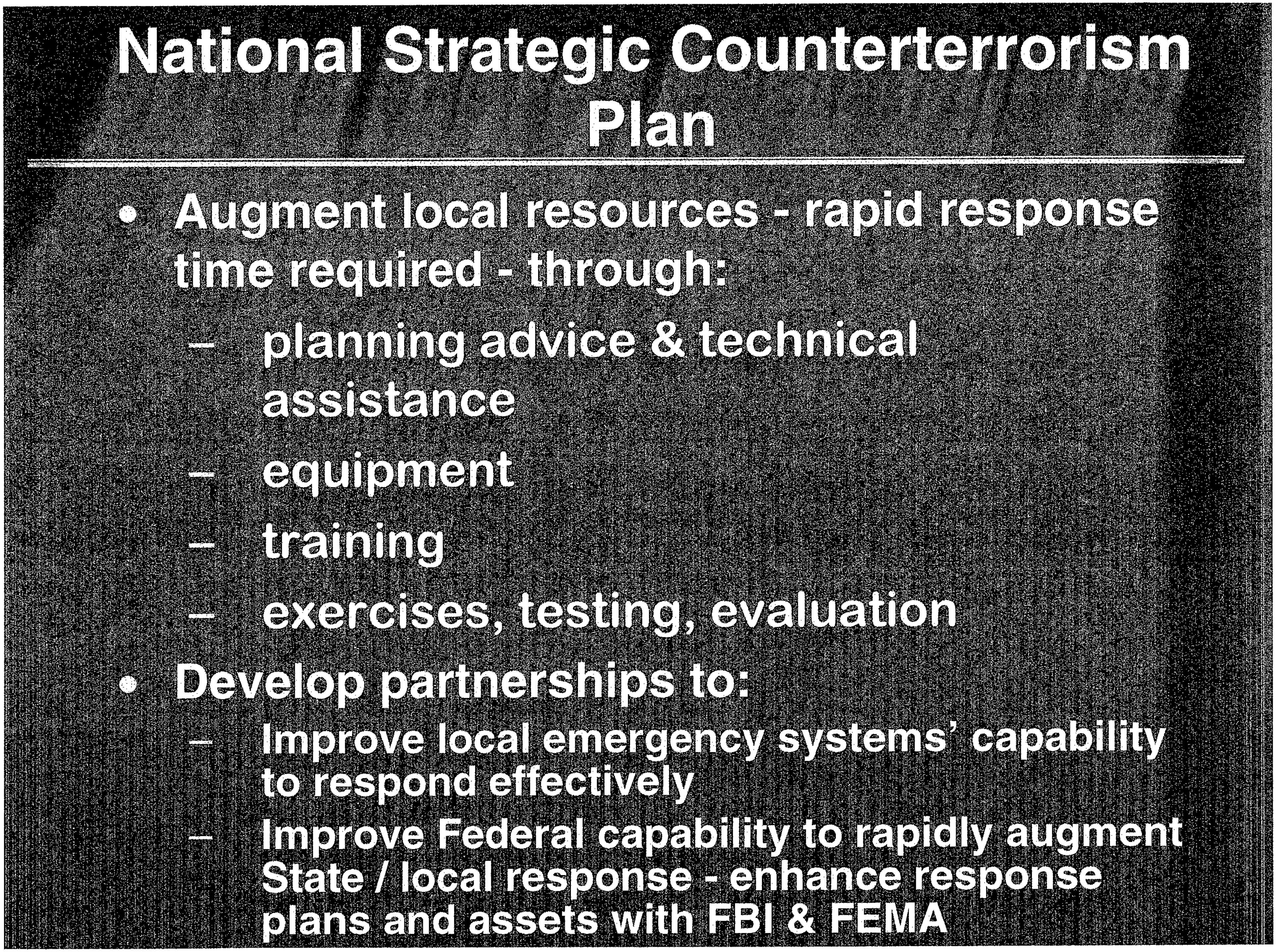
INSUFFICIENT CAPABILITIES / CAPACITY: PPE, DETECTION, & DECON

AMBULANCE TRANSPORTS
CONTAMINATED
CASUALTIES
SECONDARY EXPOSURE
TO 1ST RESPONDERS
INSUFFICIENT MEDICAL MGMT
INSUFFICIENT ANTIDOTE

NO DECON CAPABILITY
ER & HOSPITAL
CONTAMINATED
INSUFFICIENT Rx
NEED FOR CONSULTATION



Crisis Management → Consequence Management

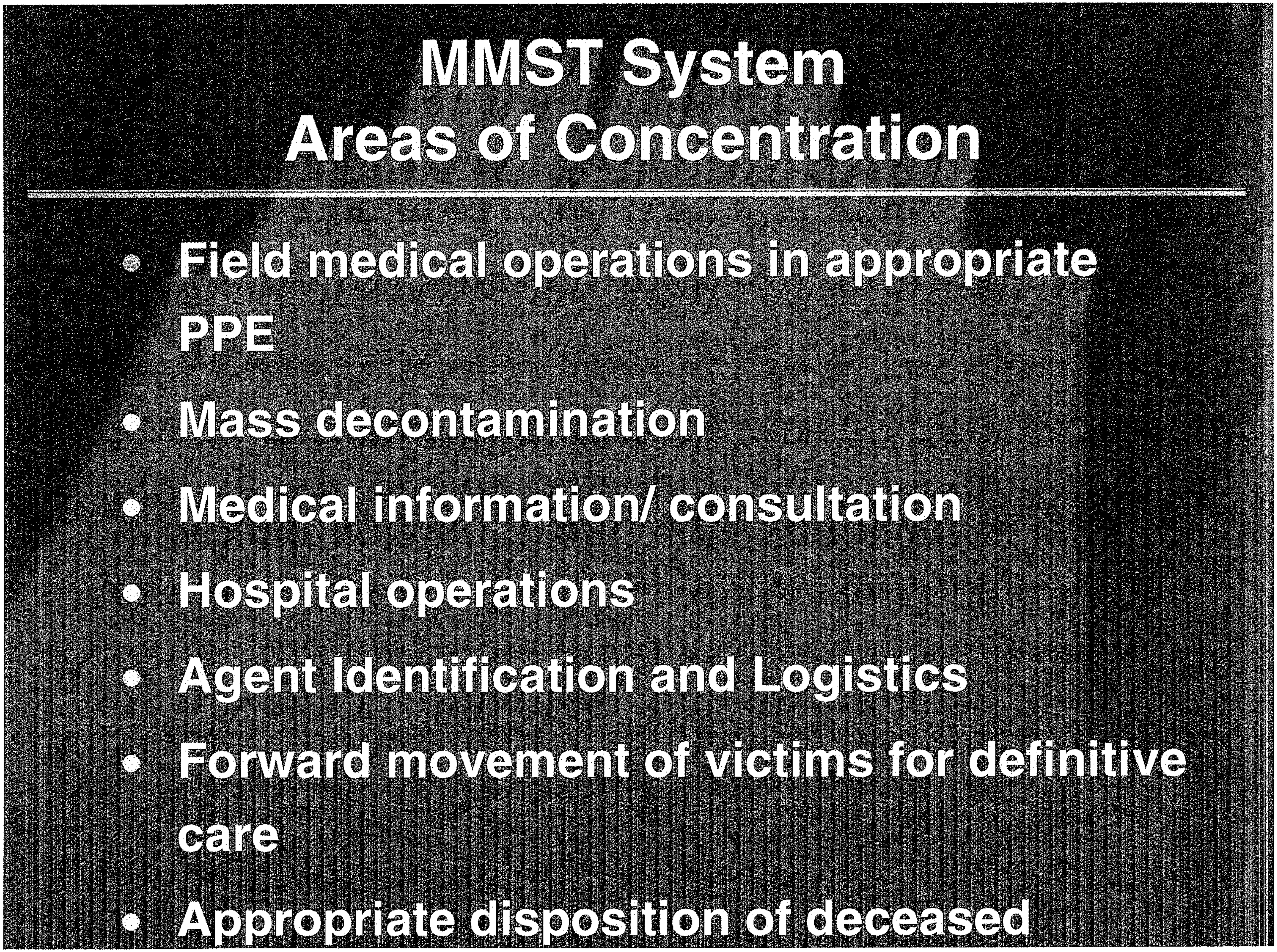


National Strategic Counterterrorism Plan

- Augment local resources - rapid response time required - through:
  - planning advice & technical assistance
  - equipment
  - training
  - exercises, testing, evaluation
- Develop partnerships to:
  - Improve local emergency systems' capability to respond effectively
  - Improve Federal capability to rapidly augment State / local response - enhance response plans and assets with FBI & FEMA

Metropolitan Medical Strike Team System [MMSTs] Emphasis

- To enhance local planning and response systems capability, tailored to each city, to care for victims of a terrorist incident involving a weapon of mass destruction
- Characteristics
  - Concept of Operations Plan
  - Specially trained responders
  - Special pharmaceuticals
  - Detection, PPE, decontamination, communication, and medical equipment and other supplies
  - Enhanced emergency medical transport & emergency room capabilities

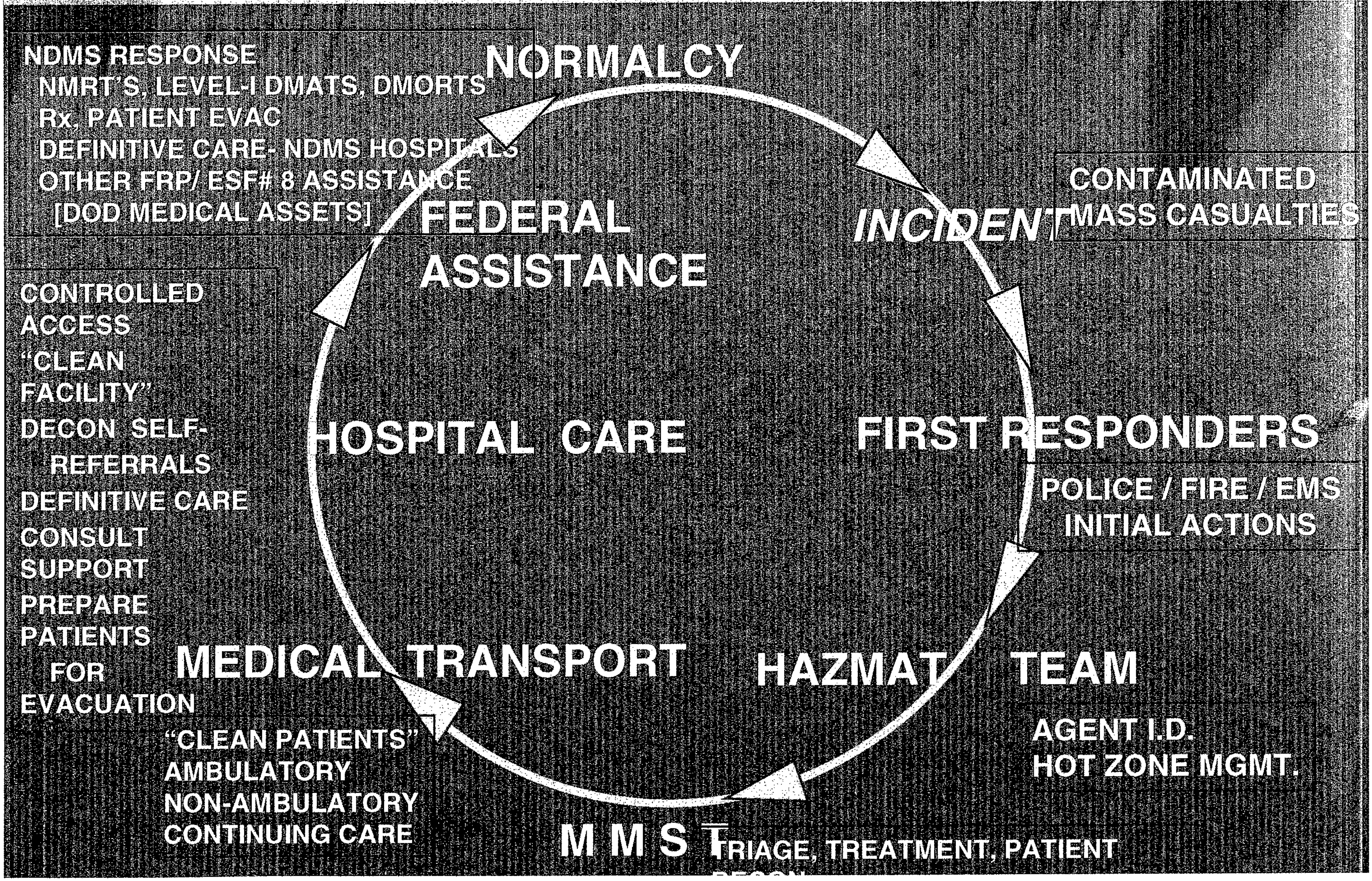


MMST System
Areas of Concentration

- Field medical operations in appropriate PPE
- Mass decontamination
- Medical information/ consultation
- Hospital operations
- Agent Identification and Logistics
- Forward movement of victims for definitive care
- Appropriate disposition of deceased

INCIDENT LIFE CYCLE

SYSTEMS APPROACH WITH PREPAREDNESS



NORMALCY

INCIDENT

CONTAMINATED MASS CASUALTIES

FIRST RESPONDERS

POLICE / FIRE / EMS INITIAL ACTIONS

HAZMAT TEAM

AGENT I.D.
HOT ZONE MGMT.

M M S TRIAGE, TREATMENT, PATIENT

MEDICAL TRANSPORT

"CLEAN PATIENTS"
AMBULATORY
NON-AMBULATORY
CONTINUING CARE

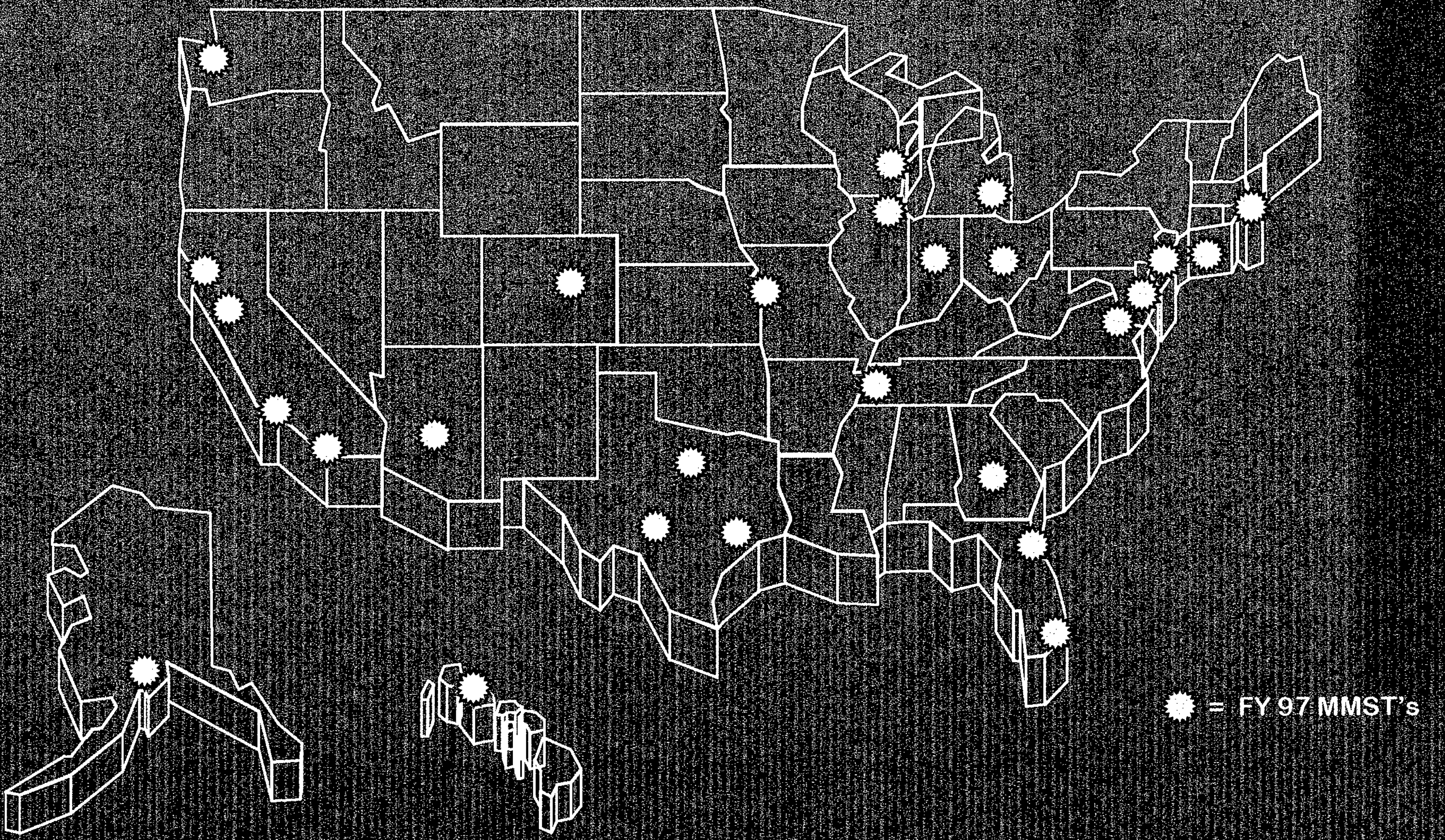
HOSPITAL CARE

CONTROLLED ACCESS
"CLEAN FACILITY"
DECON SELF-REFERRALS
DEFINITIVE CARE
CONSULT
SUPPORT
PREPARE PATIENTS FOR EVACUATION

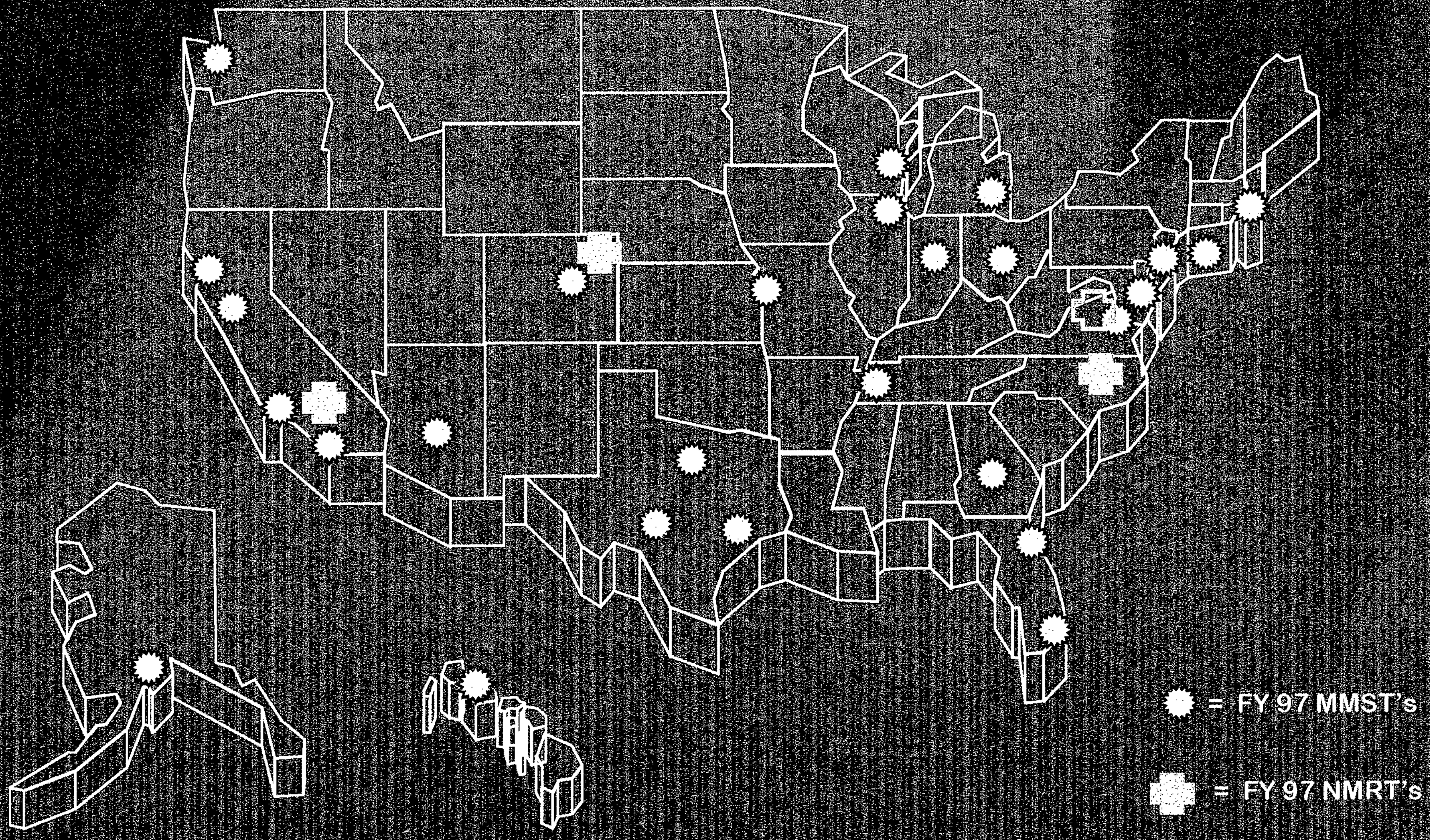
FEDERAL ASSISTANCE

NDMS RESPONSE
NMRT'S, LEVEL-I DMATS, DMORTS
Rx, PATIENT EVAC
DEFINITIVE CARE- NDMS HOSPITALS
OTHER FRP/ ESF# 8 ASSISTANCE
[DOD MEDICAL ASSETS]

Cities Developing MMSTs - 1997



Cities Developing MMSTs / NMRTs - 1997



Department of Defense

Domestic Preparedness Support

for Weapons of Mass Destruction

Director of Military Support

Agenda

- DOMS Responsibilities and Roles
- Disaster Response
- Domestic Preparedness
- DoD WMD Incident Response
- Reserve Component (RC) Consequence Management Response

Executive Agent Mission

The Secretary of Defense directs the Secretary of the Army to act as the DoD Executive Agent to plan for and commit DoD resources in response to requests from Civil Authorities.

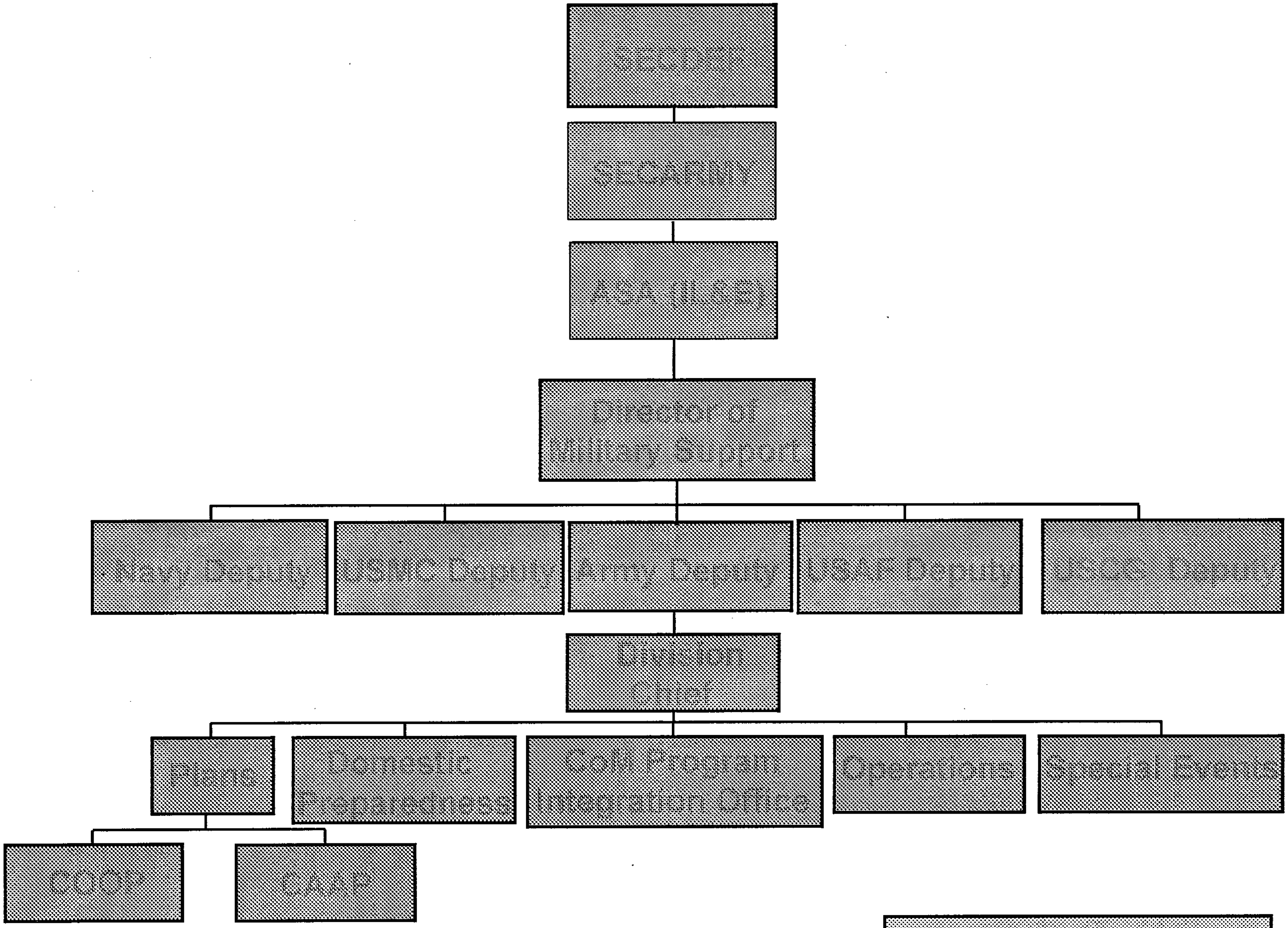
- **Military Support To Civil Authorities (MSCA)**
- **Military Assistance For Civil Disturbances (MACDIS)**
- **Special Events**
- **Domestic Preparedness Training Program**
- **Consequence Management Program Integration Office**
- **Critical Asset Assurance Program (CAAP)**
- **Continuity Of Operations Program (COOP)**

Director of Military Support

Director of Military Support

- Serves as the Secretary of the Army's Action Agent
- Tasks Services, CINCs and Defense agencies
- Unique chain of command

DOMS Chain of Command



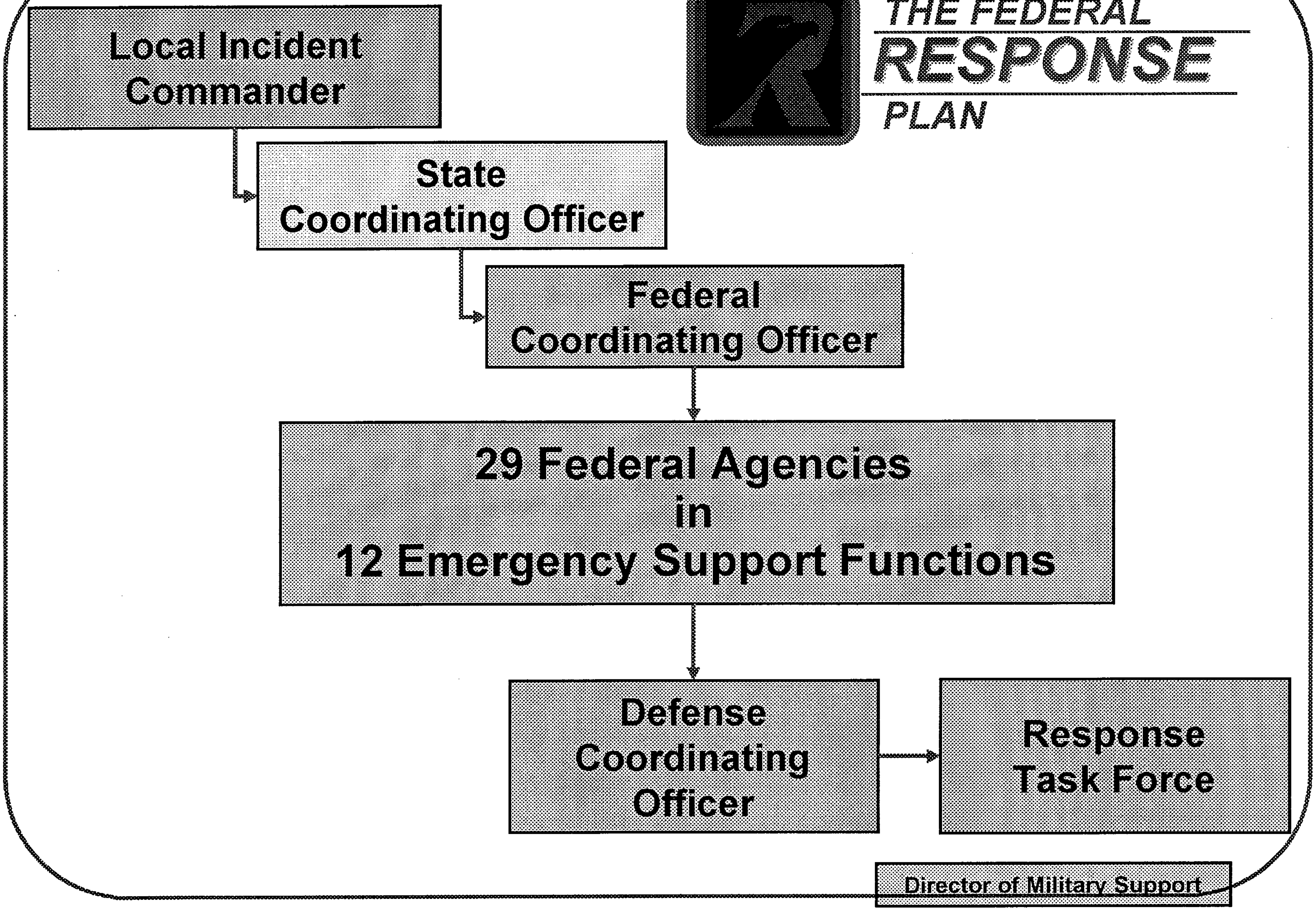
Director of Military Support

Principles

- Federal government assists state agencies
- DoD supports lead federal agencies
- DoD provides support IAW MOUs and plans
- DoD support is reimbursable
- DoD support does not compete with the civilian/commercial sector

Director of Military Support

THE FEDERAL RESPONSE PLAN



Local Incident Commander

State Coordinating Officer

Federal Coordinating Officer

29 Federal Agencies in 12 Emergency Support Functions

Defense Coordinating Officer

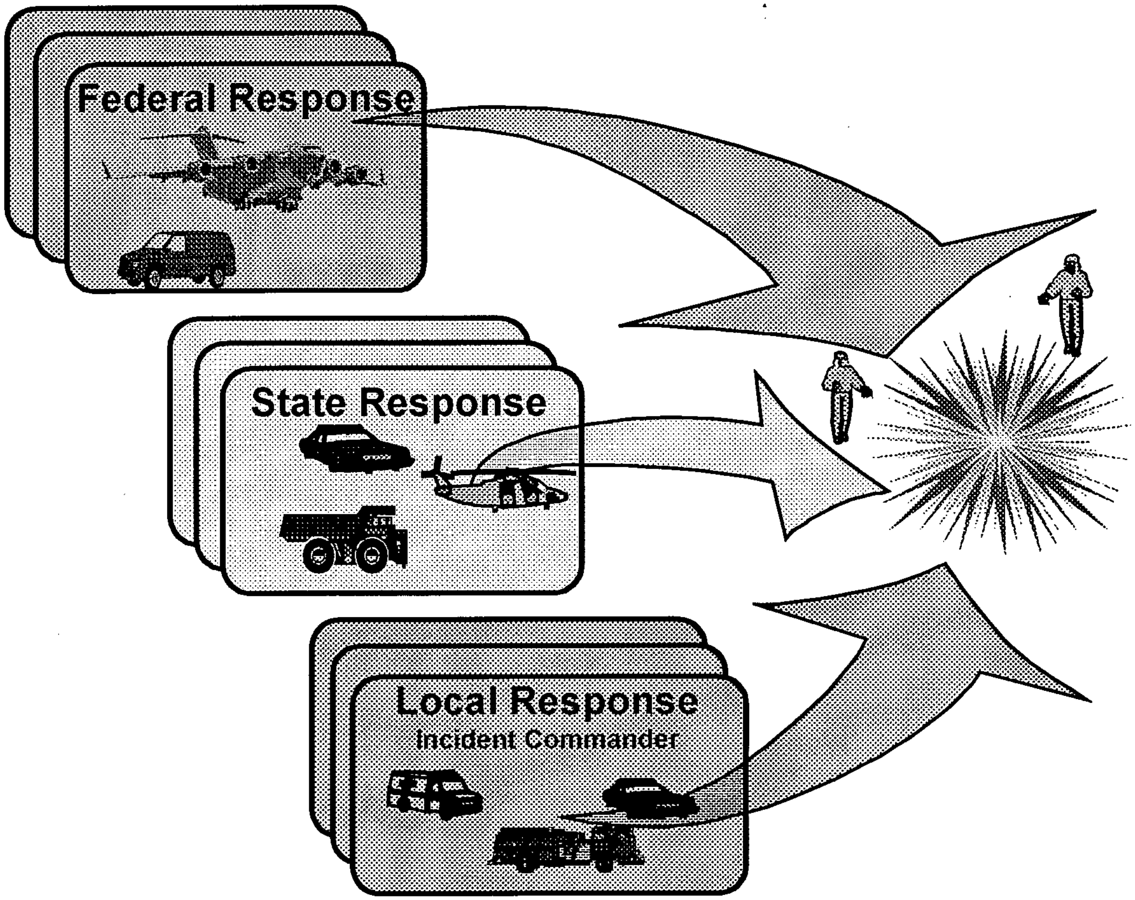
Response Task Force

Director of Military Support

Federal Response Plan

EMERGENCY SUPPORT FUNCTIONS (ESFs)	RESPONSIBLE AGENCY	DOD POC
1. TRANSPORTATION	DOT	CINCTRANS
2. COMMUNICATIONS	NCS	OASD(C31)
3. PUBLIC WORKS & ENGINEERING	DOD	USACE
4. FIREFIGHTING	USDA	FORSCOM
5. INFO & PLANNING	FEMA	DOMS
6. MASS CARE	RED CROSS	DLA
7. RESOURCE SUPPORT	GSA	DLA
8. HEALTH/MEDICAL SERVICES	DHHS	FORSCOM
9. URBAN SEARCH & RESCUE	FEMA	DOMS
10. HAZARDOUS MATERIALS	EPA	NAVY, SUPV SALV
11. FOOD	USDA	DLA
12. ENERGY	DOE	USACE

Tiered Disaster/Emergency Response



- Full response requires local, state, and federal assets
- State response includes National Guard
- Military support requires Total Force involvement

Director of Military Support

Immediate Response

Commanders, in imminently serious conditions, take actions to:

- Save lives
- Prevent human suffering
- Mitigate great property damage

When conditions & time do not permit approval from higher headquarters

Must inform DoD Executive Agent through chain of command

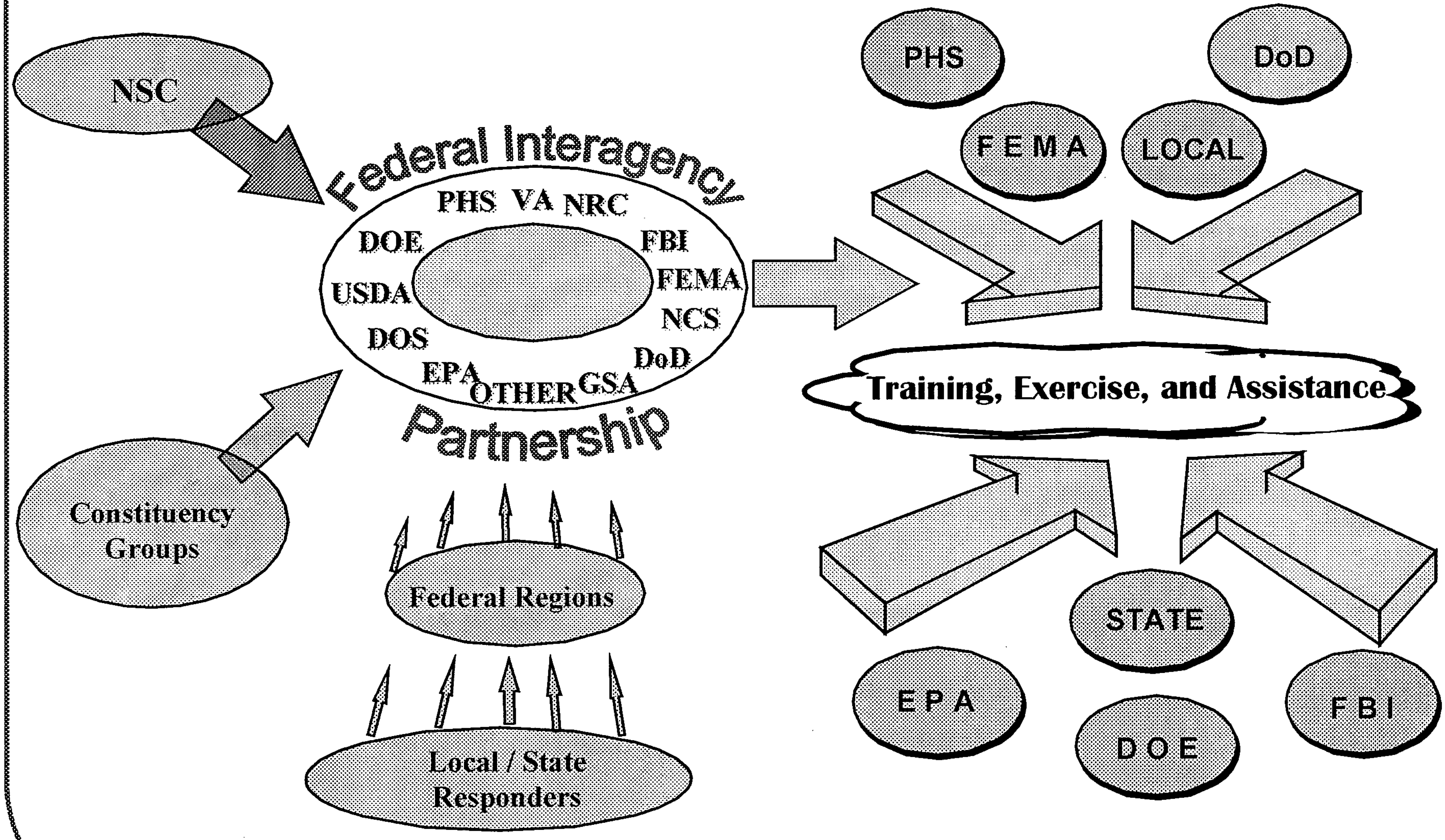
Purpose of Nunn-Lugar-Domenici Act

- To enhance the capability of the Federal Government to prevent and respond to terrorist incidents involving weapons of mass destruction.

- To provide enhanced support to improve the capabilities of state and local emergency response agencies to prevent and respond to such incidents at both the national and local levels.

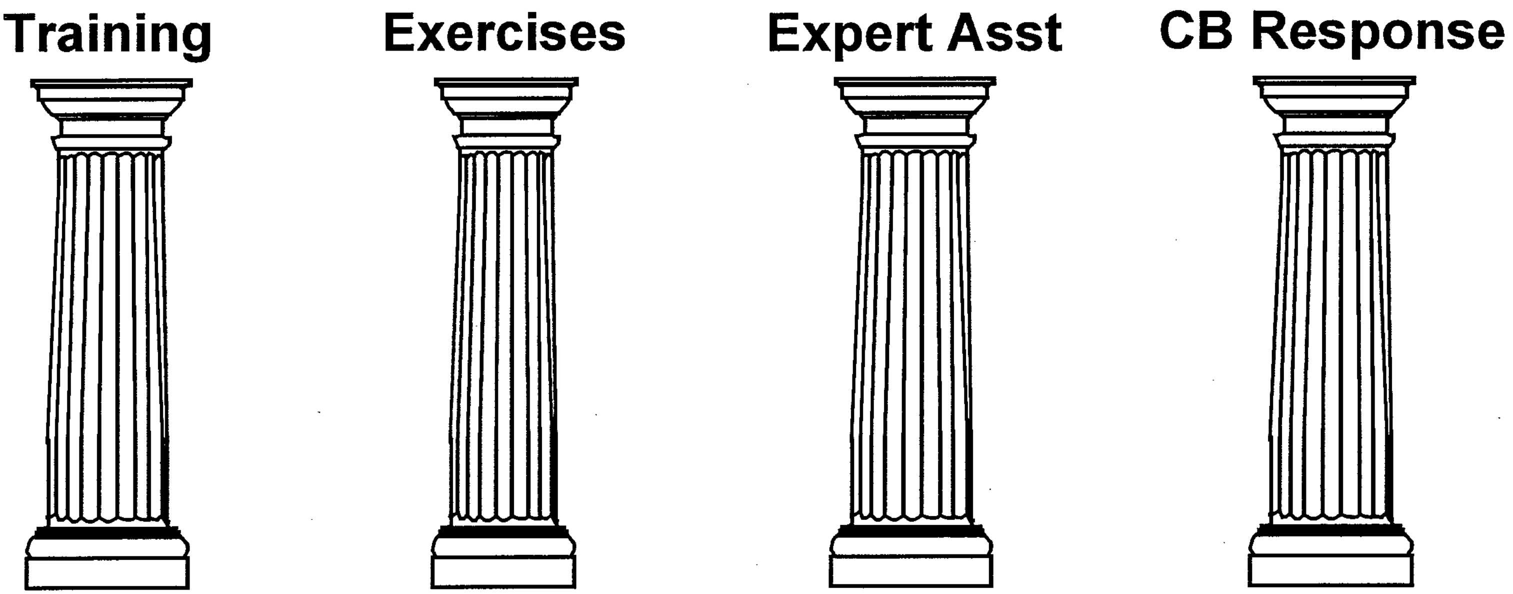
IMPLEMENTATION PARTNERSHIP

Federal, State, and Local



Director of Military Support

Pillars of Domestic Preparedness



Training

- Fire
- Law
- Medical
- Operators/ Dispatchers
- Senior Elected Officials

Exercises

- Table top
- Functional
- Annual

Expert Asst

- Hotline
- Helpline
- PPE Testing
- Web Page

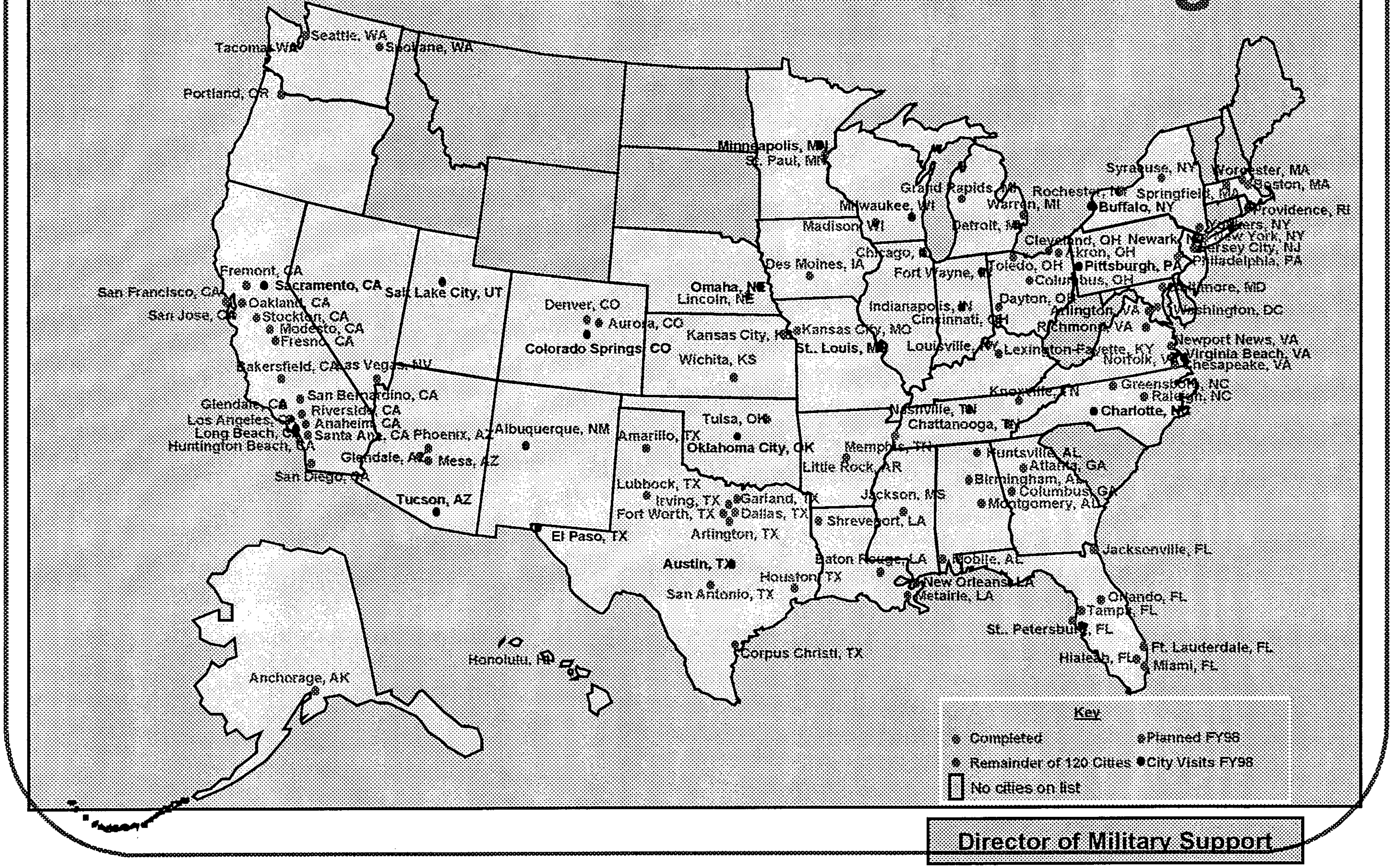
CB Response

- Specialized DoD Assets

Builds Upon Existing OSHA Infrastructure

Director of Military Support

Cities Scheduled For Training



Director of Military Support

Federal Government Response Assessment WMD Scenarios

It's not a question of IF, It is a question of WHEN and WHERE?

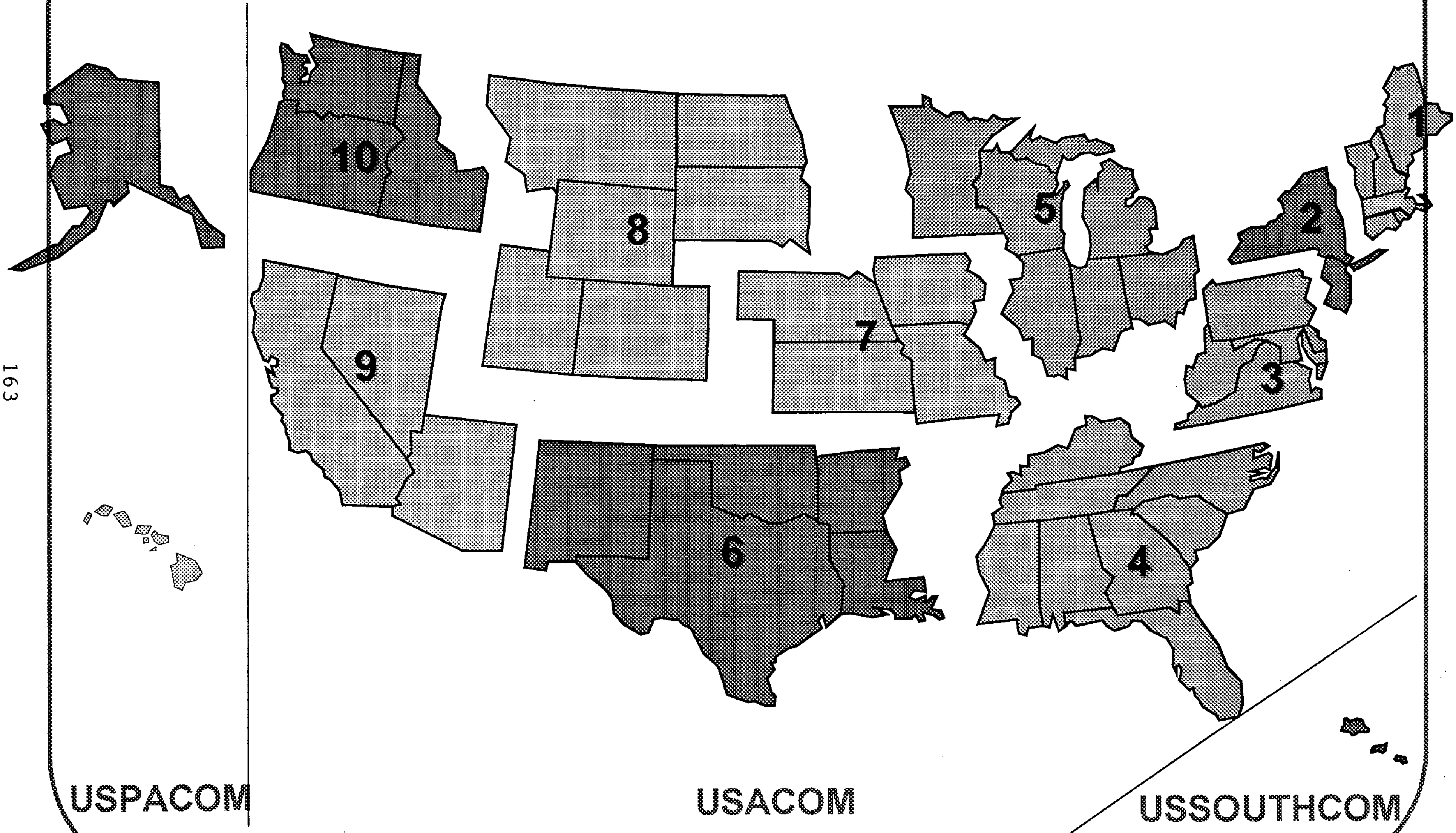
Scenario	Capacity	Command	Communications	Equipment	Information	Logistics	Plans	Overall
Radiological Threat (Plutonium)	●	◍	○	●	●	●	○	●
Summary: Terrorists place a radiation dispersal device which distributes plutonium over a populated area.								
Nuclear Explosion Threat (Uranium)	●	◍	○	●	●	●	○	●
Summary: An improvised nuclear device (1.5KT) is exploded at midday in the vicinity of a state capitol building.								
Biological Agent Threat (Anthrax)	●	○	○	●	●	●	●	●
Summary: 100 grams of anthrax released into the air distribution system at a major airport.								
Chemical Nerve Agent Threat (GB)	●	◍	○	●	●	●	○	●
Summary: 10 gallons of Sarin is released on a busy morning in trash canisters at 5 subway stations in a major city.								
Chemical Nerve Agent Threat (VX) (Persistent)	●	◍	○	●	●	●	○	●
Summary: M23 land mines (.8lb) placed in suitcases at major airport and exploded at midday								

* Bottom Line - we are not ready!

Crisis and Consequence Management Definitions

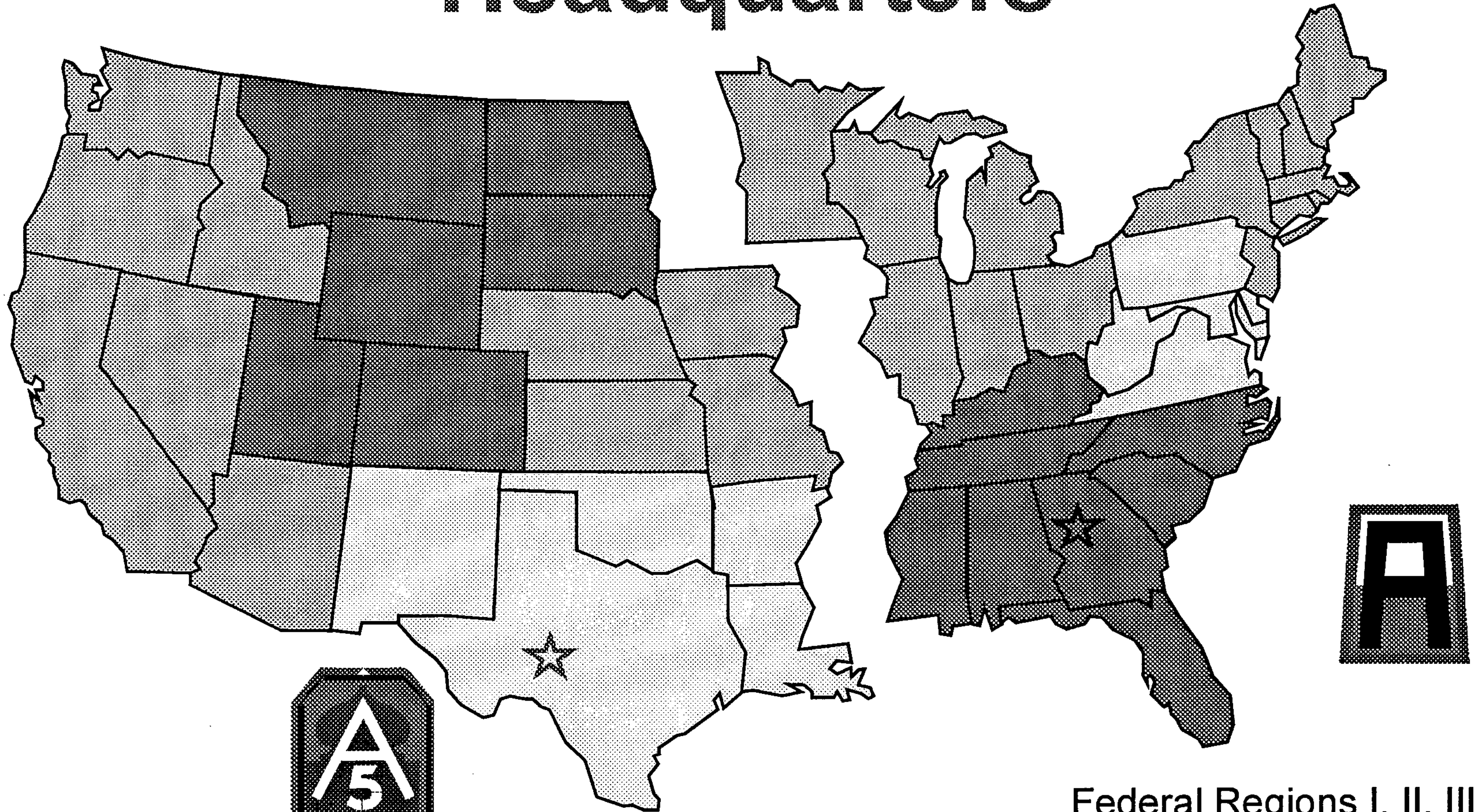
- Crisis Management
  - Measures to anticipate, prevent, and/or resolve a terrorist threat or incident
    - Primary Responsibility for Federal Response
    - Lead Federal Agency: FBI
- Consequence Management
  - Measures to alleviate the damage, loss, hardship, or suffering caused by incident
    - Primary Responsibility: State/Local Government
    - Lead Federal Agency: FEMA, coordinating Federal Consequence Management support to the state

Supported CINCs



Director of Military Support

Response Task Force Headquarters



Federal Regions VI, VII,VIII, IX, X
21 States

Federal Regions I, II, III, IV,V
27 States, DC

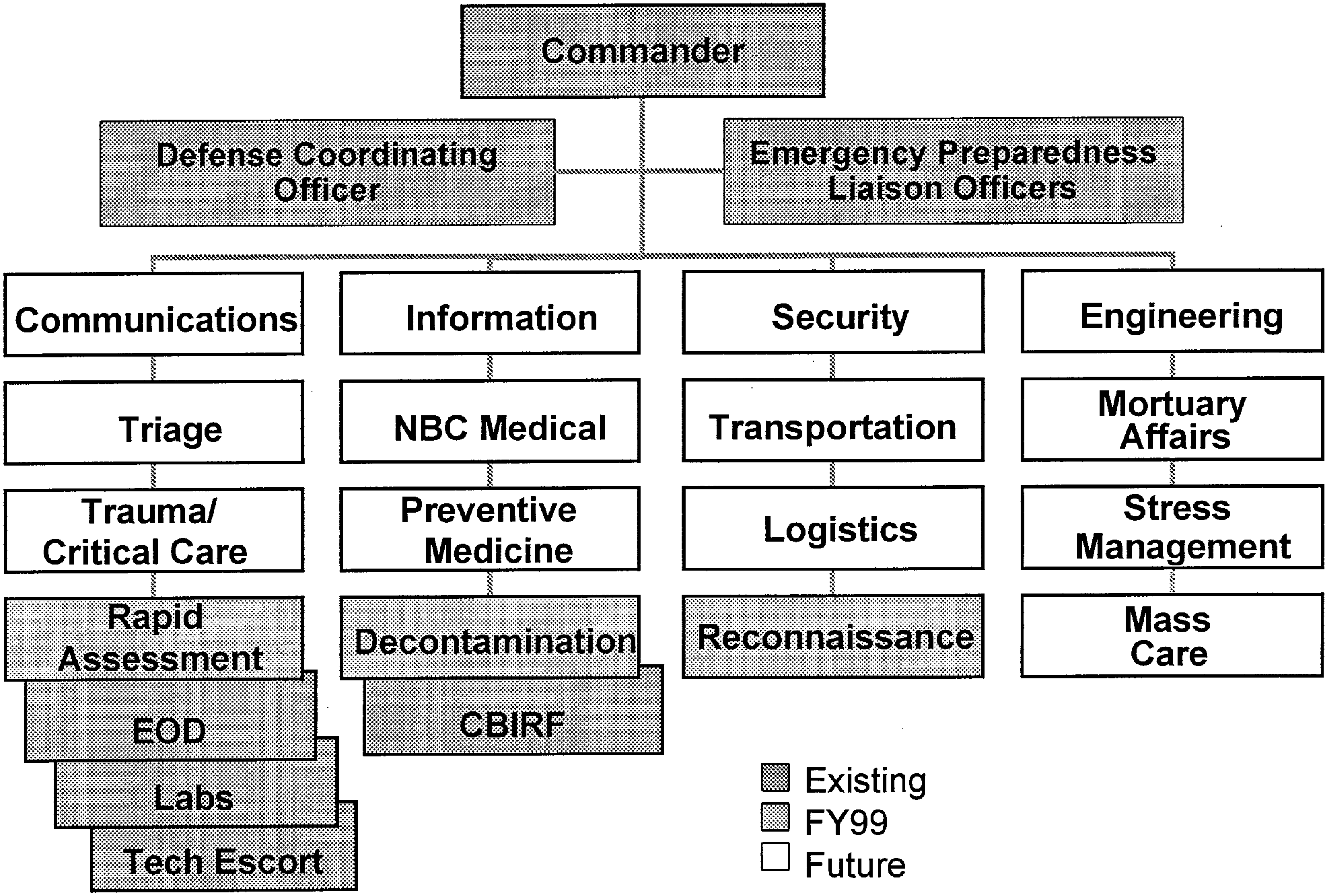
Director of Military Support

Operational Objectives

> "It's hard to deal with something until you know what you have. We need the Feds to tell us what we're dealing with."
>
> *-Typical First Responder Comment*

- Provide a DoD response capability to supplement local, state, and federal assets responding to WMD attacks.
- Optimize DoD's ability to aid civil assessment of WMD events by locating National Guard teams in each state and territory, available for use in that jurisdiction.
- Effectively use Reserve assets as part of DoD's response to assist civil authorities in responding to WMD attacks.

Response Task Force Elements



▩ Existing
▨ FY99
□ Future

Director of Military Support

Reconnaissance

Mission

- Search, Survey and Sample
  - Find safe areas
  - Rescue victims

Units Employed

- Army Chemical Units
- 28 elements in FY99
- 55 elements by end of FY00

Decontamination

Mission

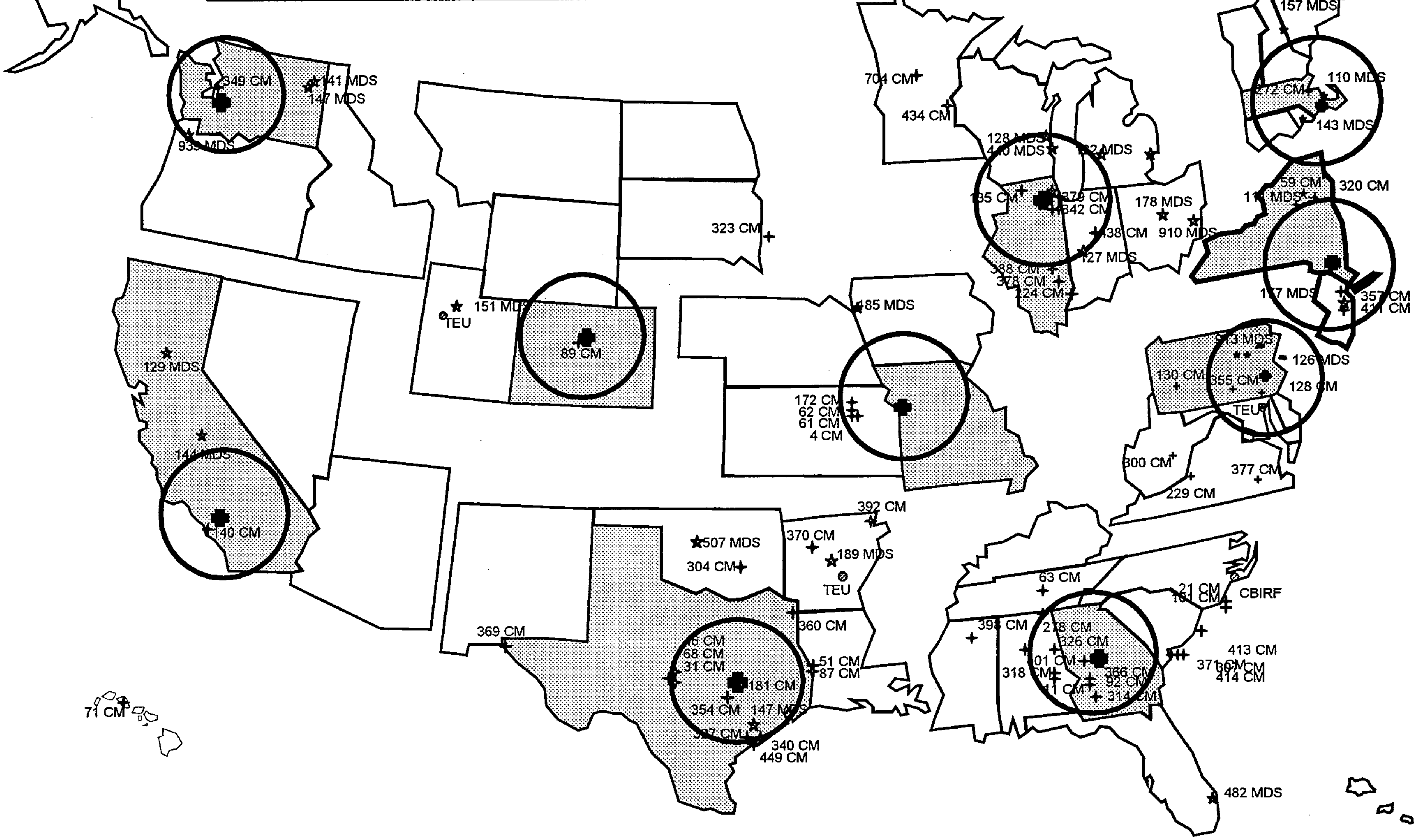
- Decontaminate Victims
  - Incident Site
  - Hospitals

Units Employed

- Army Chemical Units
- Air Force Patient Decontamination Teams
- 127 elements by end of FY00

Director of Military Support

FY99 Implementation

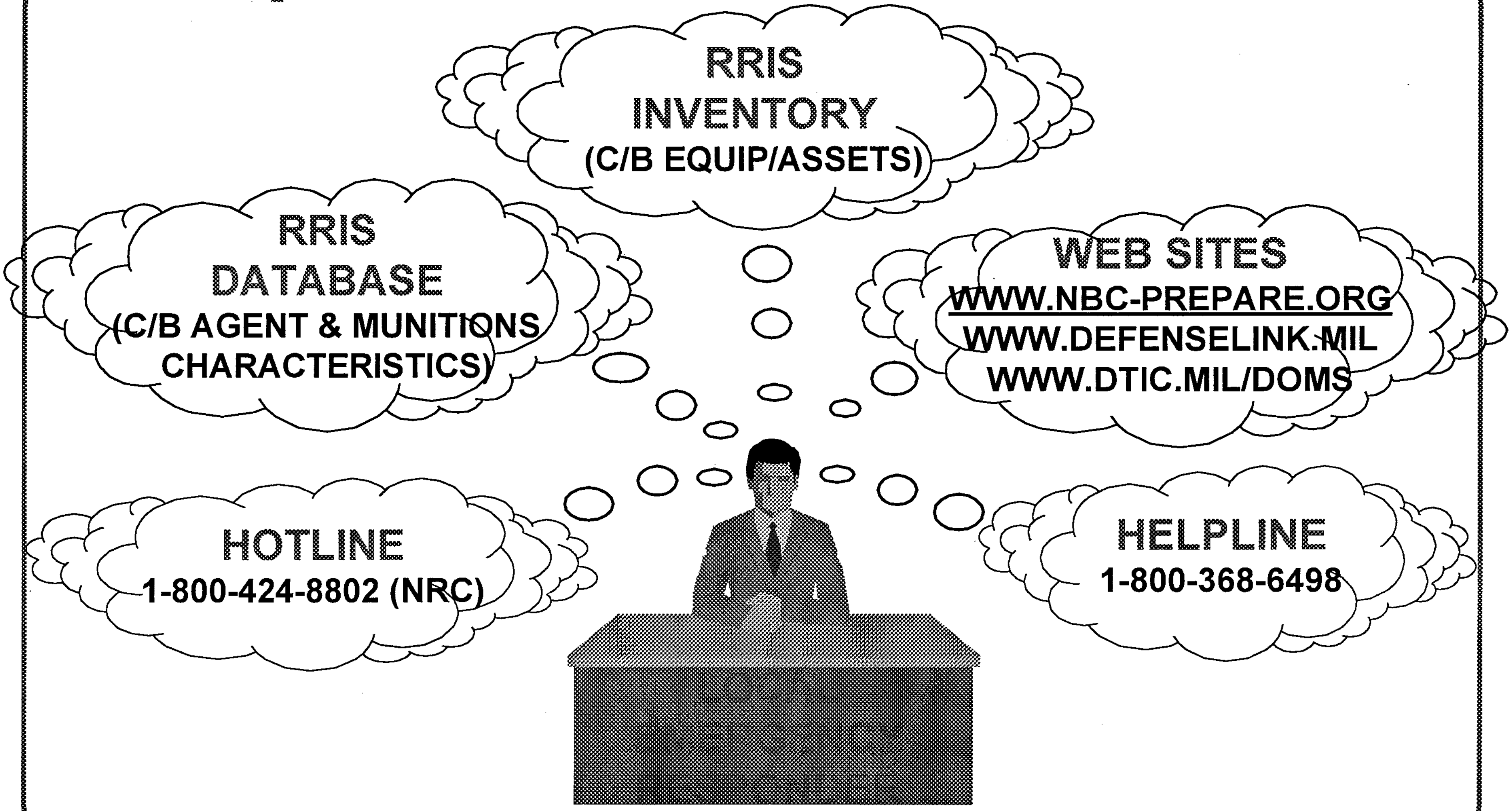


Program Overview

Element	Military Personnel Trained and Equipped		
	FY99	FY00	Total
Rapid Assessment	220	+	220+
Decontamination	1270	1270	2540
Reconnaissance	550	550	1100
Medical	100	100+	200+
Other Elements	0	+	+
Total	2140	1920	4060+

Director of Military Support

Expert Advice & Assistance



RRIS
INVENTORY
(C/B EQUIP/ASSETS)

RRIS
DATABASE
(C/B AGENT & MUNITIONS
CHARACTERISTICS)

WEB SITES
WWW.NBC-PREPARE.ORG
WWW.DEFENSELINK.MIL
WWW.DTIC.MIL/DOMS

HOTLINE
1-800-424-8802 (NRC)

HELPLINE
1-800-368-6498

Director of Military Support

Summary

- DoD usually supports a lead agency
- SECARMY is the DoD Executive Agent
- DOMS is the action agent
- DoD possesses a myriad of capabilities for disaster relief
- DoD is dedicated to providing a rapid and effective response

Cost and Performance Analysis of Conceptual Designs of Physical Protection Systems

M. J. Hicks, M. S. Snell, J. S. Sandoval, C. S. Potter
P. O. Box 5800
Sandia National Laboratories[†]
Albuquerque, NM 87185-0759
Phone (505) 844-7806 FAX (505) 844-0011 e-mail: mjhicks@sandia.gov

Abstract

CPA — Cost and Performance Analysis — is a methodology that joins Activity Based Cost estimation with performance-based analysis of physical protection systems. CPA offers system managers an approach that supports both tactical decision making and strategic planning. Current exploratory applications of the CPA methodology are addressing analysis of alternative conceptual designs. Hypothetical data is used to illustrate this process.

1 Introduction

Analysis of the cost and performance effectiveness of design alternatives is essential to a systems approach to physical security. While the concept of analysis of costs and performance is straightforward, implementation can be at the least tedious and, for complex designs and alternatives, can become nearly intractable without the help of structured analysis tools. CPA — Cost and Performance Analysis [1] — is a prototype integration of existing PC-based cost and performance analysis tools: ACEIT[1] (Automated Cost Estimating Integrated Tools) and ASSESS[2] (Analytic System and Software for Evaluating Safeguards and Security). ACEIT is an existing DoD (U. S. Department of Defense) PC-based tool that supports cost analysis over the full life-cycle of a system; that is, the cost to procure, operate, maintain and retire the system and all of its components. ASSESS is an existing DOE (U. S. Department of Energy) PC-based tool for probabilistic analysis of performance of physical protection systems designed for nuclear assets [2,3,4]. Two new tools are being developed: CATSS and PERFORM. CATSS (Cost Analysis Tool for Security Systems) [5] is being built around ACEIT. PERFORM, a performance data postprocessor, will integrate results generated by ASSESS and other performance analysis tools such as JTS (Joint Tactical Simulation). CPA is the over-arching architecture that aligns life-cycle costs with metrics of system and subsystem performance. The objective is to provide a tool that manages the life-cycle

[†] Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United Stated Department of Energy under Contract DE-AC04-94AL85000.

[1] ACEIT was developed by Tecolote Research, Inc. for the Electronic Systems Center, Cost Analysis Directorate, ESC/FM, Hanscom AFB, MA.

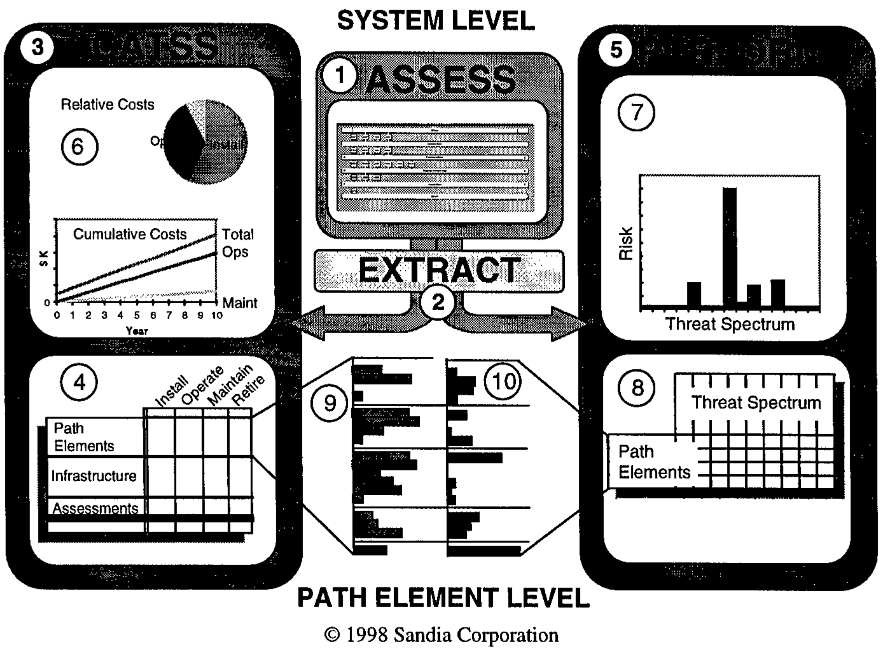
[2] ASSESS was developed for DOE by Lawrence Livermore National Laboratory and Sandia National Laboratories.

costs of security components and activities (Activity Based Costing), and then correlates costs with probabilistic metrics of performance in a format that facilitates both operational and strategic management decisions.

2 The CPA Architecture

The CPA architecture is illustrated in Figure 1. ASSESS is a path performance analysis tool. An icon of ASSESS is the Adversary Sequence Diagram (ASD), illustrated by ① in Figure 1 and shown in greater detail in Figure 2. An ASD models the areas of increasing protection of a physical security system separated or connected by path elements. The path elements function as either barriers (e.g., fences or surfaces) or as entry control points (e. g., gates or portals). Typically, there are multiple safeguards at each path element and those safeguards may be technological or procedural.

Within the CPA architecture, Figure 1, the structure of the physical protection system is extracted [②] from ASSESS [①] to launch the CATSS module [③]. This structure defines the first of three groups of cost objects [④]. Results are extracted from ASSESS for post-processing in the PERFORM module [⑤]. Cost and performance metrics can be offered at several levels: system, [⑥]and [⑦], subsystem, path element, and safeguards in both tabular, [④] and [⑧], and graphical formats, [⑨ and ⑩].



© 1998 Sandia Corporation

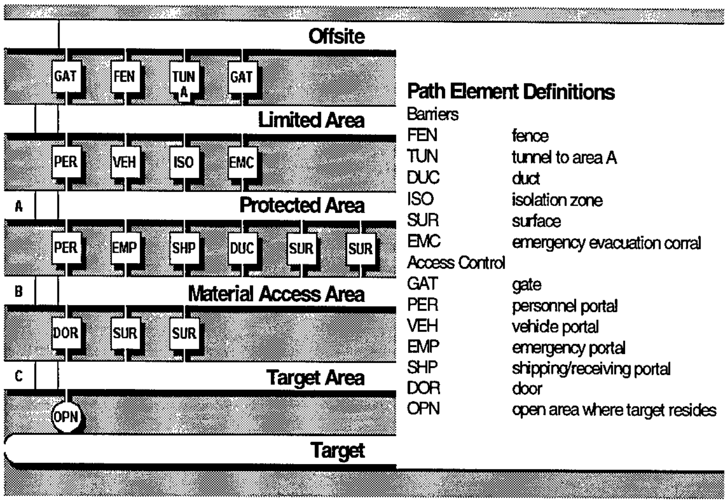
Figure 1. CPA Architecture

An ASD is a graphical representation of the physical security system.

Areas of physical protection are separated or connected by path elements.

Path elements function as
- barriers or
- entry control points.

Each path element has multiple safeguards, which may be
- technological
- procedural
- both.



Path Element Definitions

Barriers	
FEN	fence
TUN	tunnel to area A
DUC	duct
ISO	isolation zone
SUR	surface
EMC	emergency evacuation corral
Access Control	
GAT	gate
PER	personnel portal
VEH	vehicle portal
EMP	emergency portal
SHP	shipping/receiving portal
DOR	door
OPN	open area where target resides

Figure 2. Adversary Sequence Diagram (ASD)

2.1 Cost Objects and Life-Cycle Phases of Physical Security Systems

In the CATSS module of CPA, cost objects of the physical security system are grouped into three broad categories: path elements, infrastructure and labor resources, and assessments. ACEIT is the data repository and the computational engine for CATSS. ACEIT supports a variety of economic analysis tasks, including management of funding categories, phased acquisitions, inflation, and cost in now- or then-year dollars. Costs are reported over the life-cycle phases: acquisition/installation, operations, maintenance and retirement or demolition/disposal as illustrated by the Summary Costs Spreadsheet ④ in Figure 1. Costs are allocated using the principles of Activity Based Costing (ABC) [6]. The five steps of ABC are: 1) identification of the cost objects; 2) identification of the processes and activities required to produce, operate, maintain or retire the cost objects; 3) identification of the materials and labor resources required to support the processes and activities; 4) assignment of resource costs to activities; and 5) assignment of activities to cost objects.

2.1.1 Cost Objects

2.1.1.1 Path elements

The listing of path elements and safeguards implemented is mapped from ASSESS to CATSS. This allows direct alignment of costs to performance at the path element level as illustrated by ⑨ and ⑩ in Figure 1.

2.1.1.2 Infrastructure

Infrastructure refers to all those cost objects of a physical security system that cannot be assigned to specific path elements. Consider the distinction between entry control and access control. Evaluation of a credential at an entry control point is a procedural safeguard executed at a path element. Access control is an infrastructure set of procedures that may use technology to generate the credentials at some central administrative facility.

Labor resources can be both cost objects themselves and resources assigned to cost objects. Within CPA, all labor resources are initially pooled under infrastructure. When members of a resource pool perform activities associated with security at specific path elements (cost objects) or other cost objects in the infrastructure, the costs of those resources are then assigned through the activities to the path element For example, a security inspector (SI) belongs to a labor resource pool. If that SI is posted at an entry control point, then the cost of the SI is mapped to the operational costs of the path element.

2.1.1.3 Assessments (or Evaluations)

Periodic internal and external assessments of the physical security system are so critical to confidence in the integrity of the system that CPA breaks them out as separate cost objects.

2.1.2 Life-cycle Phases

The cost estimation structure offered by the Summary Costs Spreadsheet provides a balanced approach to representing costs over the full life cycle of a system from installation through operations and maintenance to demolition and disposal, thus providing a context for capturing the full cost of ownership of the system.

2.2 Performance Metrics of Physical Protection Systems

Safeguards provide detection or delay. The safeguard performance metrics are threat- and tactic-specific. These safeguard metrics roll up to threat- and tactic-specific path-element performance metrics. A fundamental principle of physical protection is that systems must first detect an intrusion and then delay the intruder long enough to allow effective response. Effective response interrupts and successfully neutralizes the intruder before he can accomplish his objective. Therefore, the threat-specific systems-level performance metrics consider detection probabilities together with delay and response times.

2.2.1 Risk

A systems-level performance metric is risk, which is defined as follows.

$$\text{Risk} = P(A) \times [1 - P(E)] \times C \qquad (1)$$

where, P(A), is Probability of Attack

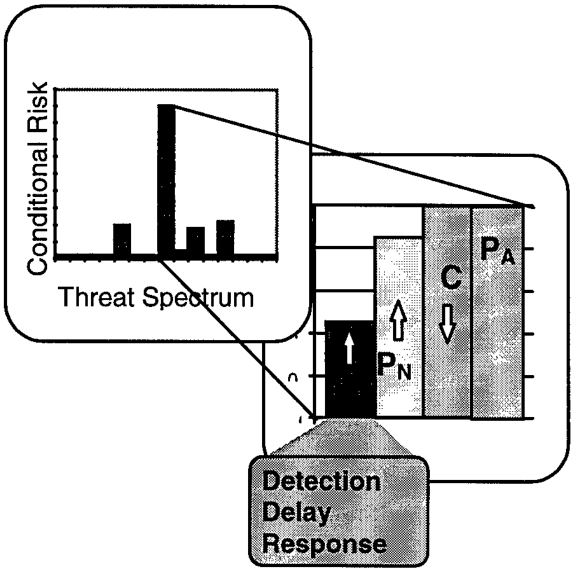
P(E), Probability of System Effectiveness, = P(I) × P(N), (2)

P(I) is Probability of Interruption,

P(N) is Probability of Neutralization,

C is Consequence.

If Probability of Attack is assumed to be one, then the performance metric is called conditional risk. Probability of Interruption is a function of the detection probabilities and delay times at the various path elements and of the time required for responders to interrupt the threat (response force time). The breakout of risk into its components is illustrated in Figure 3. Probability of Neutralization can be modeled in ASSESS and/or in JTS and should be verified with force-on-force engagement exercises. Similarly, response force times should be verified with limited-scope performance tests. Consequence may be defined by a normalized scale from zero to one or may be expressed in more absolute terms such as cost and time required to recover lost capabilities.



Risk should be reported across the threat spectrum for each target.

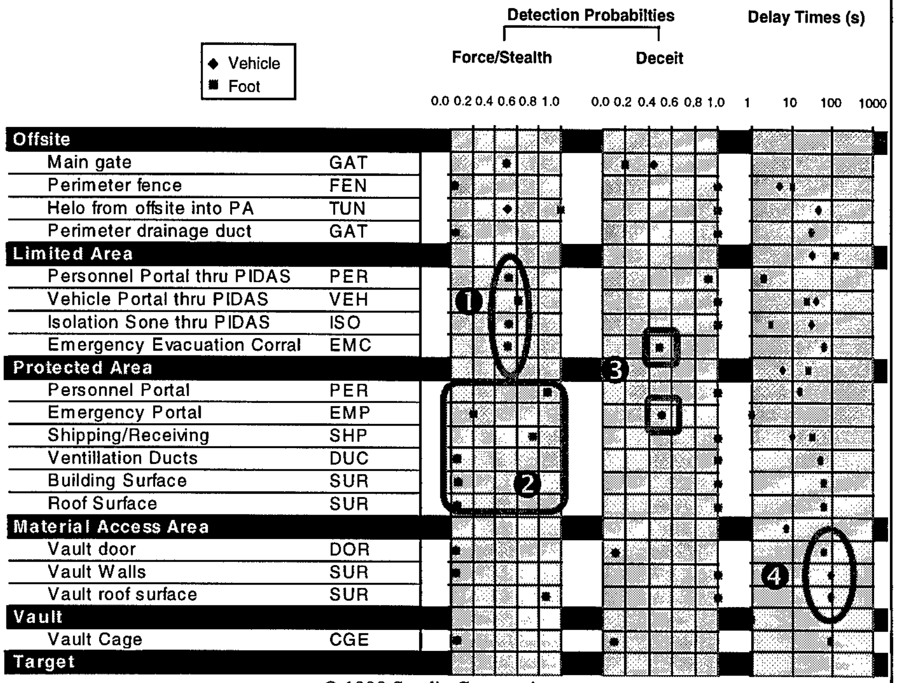
For each threat in the spectrum, conditional risk can be mitigated by:
increasing Probability of Interruption,
increasing Probability of Neutralization
and/or decreasing Consequence.

Probability of Interruption is a function of
detection,
delay and
response.

Figure 3. Breakout of Risk.

2.2.2 Detection and Delay

The PERFORM module of CPA offers decision makers systems level metrics of performance such as conditional risk across the threat spectrum, as illustrated by ⑦ in Figure 1. It allows analysts to drill down through path element and safeguard metrics of performance, ⑧ and ⑩ in Figure 1, to identify where and how technology can be used to improve performance or to control costs. The graphic illustrated by ⑩ in Figure 1 is demonstrated in Figure 4. The path elements shown in the ASD in Figure 2 are listed to the left. Path-element performance metrics (probability of detection and delay times) are shown for two modes of attack (on foot or in vehicles) and two threat tactics (force/stealth and deceit). From this figure analysts can readily examine system attributes and identify potential weaknesses. Long delays are desirable close to the target. Detection needs to occur, with high probability, before delay. Both detection and delay should be balanced. Referring to Figure 4 for the example facility, ❶ shows balanced but only moderate detection between the limited area and the protected area. ❷ shows both low and unbalanced detection. Minimum detection value at this layer is nearly zero. ❸ suggests a potential tradeoff between the requirements for security and those for safety at the emergency evacuation corral and at the emergency portal. ❹ shows balanced delay between the material access area and the vault interior.



© 1998 Sandia Corporation

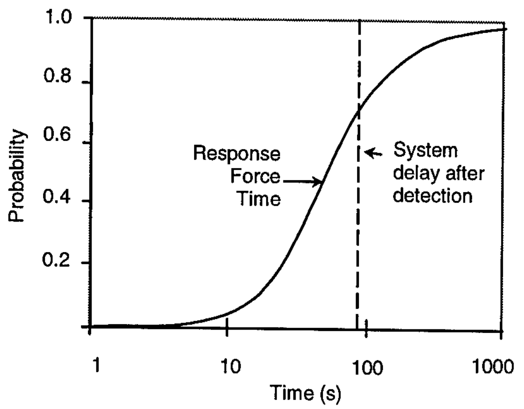
Figure 4 Metrics of path-element performance

2.2.3 Response

The example in Figure 4 shows that Probability of Detection between the limited area and the protected area is 0.5, and zero (minimum value) between the protected area and the material access area. The adversary delay is about 0.7 s across the protected area, 0 s (minimum value) at the boundary between the protected area and the material access area, about 0.7 s across the material access area and about 70 s at the boundary between the material access area and the vault. The adversary task time at the target is about 80 s.

The relationship between delay after detection and response force time for this hypothetical example is shown in Figure 5. The distribution of response force times should be determined over all possible conditions.

The data in Figure 4 and Figure 5 suggest several issues in this hypothetical design that should be addressed. 1) While detection between the limited area and the protected area is balanced, is a value of 0.5 acceptable or does it need to be increased? 2) Detection between the protected area and the material access area should either be balanced or abandoned. Detection at this layer is of particular importance if there is more than one protected area within the limited area because detection at this layer provides threat location information to the response force. This argues for balancing the detection rather than abandoning it. This same argument holds for detection between the material access area and the vault. 3) Finally, delay needs to be balanced between the protected area and the material access area. Just how much detection and how much delay are required depends on the protection objectives and the cost of improvements. To summarize, for the system as defined, a knowledgeable adversary would have a 0.5 probability of NOT being detected by this physical protection system. If detected, he has a 0.25 probability of being inside the vault before the response force arrives.



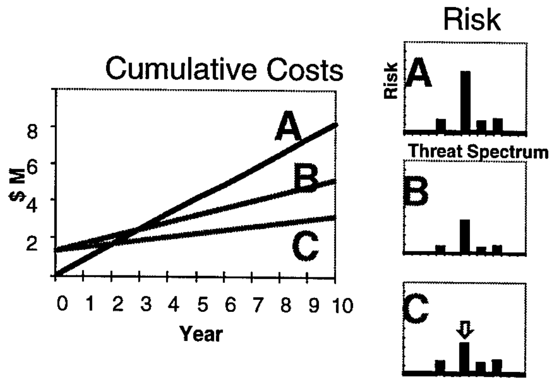
In this example, the minimum system delay for the adversary from detection at the protected area boundary to the vault cage is about 80 seconds.

25 % of the time the response arrives at the vault cage after the adversary.

Figure 5. Study of relationship between system delay and system response time

3 Cost and Performance analysis

As alternatives are identified that address the needs identified in the previous section, pertinent cost should be collected within the context of the cost estimation structure defined by the Summary Costs Spreadsheet. The costs and performance alternatives might be presented as illustrated in Figure 6. Of the three alternatives option C appears to be the best choice, provided the funds can be obtained for the initial $1.5 M installation investment. Option C would pay for itself in two years.



Option A: Do Nothing. Operations & maintenance costs accumulate at a rate of $800 K per year.

Option B Costs $1.5 M to install and $350 K per year to operate & maintain. Risk is reduced by a factor of 1.8 across the threat spectrum

Option C Costs $1.5 M to install and $200 K per year to operate & maintain. Risk is reduced by a factor of 1.8 for only one threat in the spectrum

Figure 6. Illustration of cumulative costs and associated risk profiles

4 Summary

This analysis has considered only the performance of a design, not the performance of a system as implemented. There are a number of other considerations that need to be addressed before risk can be estimated with confidence.

The CATSS module of CPA uses the principles of ABC to organize cost data by cost objects and life-cycle phases. ACEIT, the computational engine for CATSS, supports a variety of economic analysis tasks, including management of funding categories, phased acquisitions, inflation, and cost in now- or then-year dollars. The PERFORM module offers metrics of path element and safeguard performance from ASSESS analysis. It will address the integration of performance metrics from ASSESS with results from other performance analysis tools and limited-scope performance testing. The objective of CPA is to structure the collection and presentation of data in a manner that offers information in a compact form to both systems analysts and decision makers.

References

[1] M. J. Hicks, David Yates, William H. Jago, Alan W. Phillips, Dennis F. Togo, "Cost and Performance Analysis of Physical Security Systems," ADPA/NSIA 13th Annual Security Technology Symposium & Exhibition Government-Industry Exchange, June 9-12, 1997, Virginia Beach, VA.

[1] J. C. Matter, R. A. Al-Ayat & T. D. Cousins, "A Demonstration of ASSESS—Analytic System and Software for Evaluating Safeguards and Security," *Proceedings of the INMM 30th Annual Meeting,* Orlando, FL, July 1989.

[2] B. H. Gardner, Mark K. Snell & William K. Paulus, "Comparison of ASSESS Neutralization Module Results with Actual Small Force Engagement Outcomes," *Proceedings of the INMM 32nd Annual Meeting,* New Orleans, LA, July 1991.

[3] Byron H. Gardner, William K. Paulus & Mark K. Snell, "Determining System Effectiveness Against Outsiders Using ASSESS," *Proceedings of the INMM 32nd Annual Meeting,* New Orleans, LA, July 1991.

[4] David Yates, William H. Jago, Alan W. Phillips, *Cost Analysis Tool for Security Systems (CATSS), CR-0839*, Tecolote Research, Inc., 30 September 1996.

[5] Dr. Dennis Togo & Dr. Alistair Preston, "Activity-Based Cost Analysis of Security Services for a Nuclear Materials Site," prepared by Robert O. Anderson School and Graduate School of Management for Sandia National Laboratories under Contract No. DE-AC04-94AL85000, December 16, 1996.

Mission Critical Systems for Security Management

William H. Sawyer, Ph.D.

G. S. Butz, Inc.

Exton, Pennsylvania 19341

NDIA Conference

Williamsburg, Virginia

June 16, 1998

Mission Critical Systems for Security Management

Dr. William H. Sawyer, Ph.D.

Abstract

Virtually all modern security management systems use distributed processing so that the system continues to function when the CPU is down. For medium and high security applications this is not sufficient. The CPU is the critical interface between human and machine. Loss of the CPU blinds the operator to critical events and key system information. For this reason the CPU is as mission critical as the alarm panels and the intelligent door controllers. The most familiar operating systems for PC's (the preferred CPU (server) for most security management systems today) are not mission critical. Windows 95, Windows NT, OS2 and various PC versions of UNIX all can create significant data addressing problems if they fail during operation. While it is possible to recover from most of these problems, the recovery time is significant and requires a level of expertise not typically expected of a security system operator. This paper outlines the nature of these problems, suggests steps which can be taken by security managers and system designers to prevent loss of critical event notification during a significant recovery time, and outlines solutions which will greatly reduce the probability of such a problem occurring. This paper is vendor neutral. Various systems manufacturers and their attempts to address this problem are not discussed.

Mission Critical Systems for Security Management

William H. Sawyer, Ph.D.
G. S. Butz, Inc.
Exton, Pennsylvania 19341

I Introduction

Mission Critical and Security Management are terms which go together in the minds of most people responsible for the security of their facilities. Each of us has a picture in our own minds of what such a system looks like or should look like. Yet these pictures usually conflict with reality, and in some cases the picture and reality are mutually exclusive. In this paper I would like to take you through some of the issues which create these dilemmas and suggest some ways around them. The importance of these dilemmas to you and their solutions, each of which involves some type of constraint, usually money, you will have to decide.

Experience has taught us as a manufacturer that whether or not it is in the specification, every customer wants their system to run all the time no matter what the circumstance. There are no acceptable excuses. People will accept "the system is down . . . " from there is departments. They will accept it from the travel agent. They will even accept it from their bank. They cannot and will not accept it from their security management system.

At the same time each customer wants all the features of a modern computer system such as a Graphical User Interface (GUI) sometimes simply referred to as Windows. They: you, want it to run on PC's just like everything else, in fact you want it to run on your brand of PC since your company or agency has a purchasing agreement with someone and you can get it for much less than the security dealer will sell it to you.

In some cases you even want it to run on your own LAN/WAN or at least one which uses the same operating system (OS) so that your people do not need to learn two systems. (To purchase a service contract from the security vendor is to give them a license to steal.) Yet you want complete security from internal or external hackers.

These are just some of the constraints faced by us and our competitors as major security systems manufacturers today. They make UL, NFPA, and BOCA requirements seem trivial by comparison. No one, not even us, offers you the answer to all of these problems simultaneously in an inexpensive package which will fit every budget. The intent of this paper is to try to highlight some of the pitfalls and traps which are associated with the above requirements and illustrate various ways around them. Using a broad brush, we will rank the solutions we present according to their effectiveness, difficulty to implement and maintain, and initial cost. Your specific requirements may lead to a very different result.

II Security Management System Functions

Historically the two major functions of security management systems have been alarm monitoring and access control. Some years ago closed circuit television (CCTV) was added so that today most systems integrate all of these features in some way. More recently personnel management functions such as Video Badging, Time and Attendance, and Visitor Registration have been added to these systems. See Figure 1. Today many manufactures are adding low voltage lighting control, HVAC, and system maintenance management capabilities to their systems. In the future it is likely that at least certain forms of communication will also be included. The impetus to do this has come from many directions:

- The recognition that each of these areas has a critical security component,
- There can be a resulting operating cost reduction,
- There can be an increase in overall system reliability if these new functions are implemented using the design architecture developed by the security industry,
- The increasing requirement by customers for security systems to have an open architecture which has led to the implementation of some features of the BackNet protocol and LON Works.
- The increased requirement for mission critical secure communications with system analysis which will record, track, and analyze attempted security breaches.
- In order to simplify training, operation, and maintenance, there must be a similar look and feel to each system.

III The need for mission criticality

It is intuitively obvious that the systems above should all be hardened against failure. They should be able to remain operational under the most difficult of circumstances. Lightning, critical component failure, CPU failure, and operator error, to name a few should not be able to compromise or bring the system or any one of its major components down.

The security industry recognized this early in its career. Battery backup and un-interruptible power supplies (UPS) have always been available. Distributed processing was introduced in the early 1970s with the advent of microprocessors which made possible intelligent local controllers. Redundant communication schemes and two ended loop communications were introduced at nearly the same time. Software which drove the intelligent controllers in these systems was written in the assembly code native to the microprocessor which was the heart of the system. It was a forgone conclusion that this code had to be written in such a way that it did not crash. In addition, should the microprocessor itself experience a glitch, a "watchdog" circuit could immediately reboot the system without loss of data and the entire operation could continue. Files could be updated in real time and the system's data and logs could be backed up without the need to interrupt the system's operation.

These were the days of the Z80, CPM, and later DOS. As good as they were, there were serious limitations. Systems were slow, the sizes of the systems were limited by the constraints of DOS, the cost of memory, and in general they were effectively single user systems. Such features as multiple users and multitasking were at best in the realm of minicomputers which pushed the cost of such systems out of reach of most potential users. Perhaps more important was the fact that every system was different. In many cases even an upgrade from the same manufacturer was incompatible with the previous release of the system.

The development of new operating systems for the PC led to many advances in the security industry. Notable among these were the advent of multiuser, multitasking operating systems and 32 bit internal and external bus architecture. But nothing was to change the landscape as much as the advent of Microsoft Windows in its various versions from Windows 3.1 to Windows 95 and Windows NT. For Microsoft the intent was to provide the PC user with an intuitive, easy-to-use man/machine interface similar to the one so successfully marketed by Apple Computer. Success was swift. The public liked the product and Windows 3.x quickly replaced DOS and its competitors as the PC operating system of choice, even though it ran on top of DOS. Windows 3.x had many serious limitations however which kept it from entering the serious security systems market. It offered virtually no file security, it was not a true multitasking operating system, and it was prone to periodic and unpredictable failures.

The rest of the computer market also became quickly aware of Windows 3.x limitations. Microsoft already had an answer in preparation: Windows NT for network and large system users, and Windows 95 for everyone else. Much effort was put into the development of Windows NT. Among the central design features were the requirements to meet the stringent demands of the Federal Governments C2 and C3 security requirements, and the need for portability which would allow the system to run on many different computers and architectures. Much of this development took place in the early 90s when 16 bit internal architecture and 8 bit and 16 bit external architectures were in general use.

In order to accommodate these and other requirements, compromises inevitably had to be made. Among these was the loss of mission criticality. The most obvious manifestation of this is the requirement to go through a shut down procedure when you want to turn off a computer using either Windows 95 or Windows NT. Where DOS was an extremely robust operating system rarely suffering a fatal failure, Windows in all its versions has been subject to fatal failures many of these as a result of its memory utilization scheme. If a DOS program did fail, it was possible to reboot the system immediately. If any data was lost, it was only that which was being written to the disk at the time of the interruption. As you all have painfully experienced at one point or another, such is not the case with Windows. When it is restarted, at best the system must go through the procedure of reexamining the hard disk files while it rebuilds the file allocation table or its equivalent.

Let me assure you. This paper is not a plea for the "good old days" of DOS. We are far better off today than we were even two years ago. Rather it is my intent to point out some of the design limitations of current systems and offer you the security system user suggestions which will allow you to overcome them in your system design. As examples, let us examine two of these compromises and their impact on the mission criticality of the modern security management system.

1 Memory allocation schemes:

a. Fixed Partitioning (Figure 2a): In this case a specific region of memory is assigned to each program which should be sufficient for all of its requirements. In some variations where there are large memory requirements, paging may be used where portions of the program or its data file are kept on disk and only that information which is currently required is kept in memory.

Fixed partitioning can be done manually when the system is setup, either by the program when it is started, or by the operating system itself. In any case once a block of memory is allocated to a particular program, only that program and its data can reside there. In early DOS and DOS like systems the partition size was limited to 640K or less depending upon the requirements of the OS (in multitasking environments each program's memory was limited). Later systems allow access to up to several GB. The disadvantage of this scheme is its inefficient use of memory. If a program infrequently requires large amounts of memory, the maximum amount of memory it requires is none the less always allocated to it. 32 bit multitasking multi-user operating systems utilizing this type of memory allocation are UNIX, LINIX, DRDOS, and CCIDOS among others.

b. Dynamic Partitioning(Figure 2b): Here the operating system keeps track of the amount of memory each program needs and the addresses where it is located. As the programs run.and their need for memory changes, the operating system reallocates memory to each of them. Since there is rarely ever enough memory, particularly in larger systems, paging schemes are stilled employed. This is a very egalitarian method which results in highly efficient use of memory and in the case of large programs frequently a significant increase in speed.

Unfortunately the technique is not entirely fool proof. Among other problems, for example, a key location which is still needed can be written over by another program or another part of the same program, the operating system believing that the information in that location was no longer required. This error can result in the famous words "Your program has committed a fatal error . . . " Windows operating systems and the newer versions of most other operating systems utilize this technique of memory management.

2 Disk File Allocation (Figure 3): When data is stored on a disk the address or addresses of its location or locations are maintained in a table. There are various techniques for storing this data: the File Allocation Table (FAT) was used by DOS-BASED systems and some implementations in Windows. Windows NT uses the NTFS. OS/2 uses HDFS. In any case, in early DOS and DOS like systems the FAT was stored on the disk at all times and updated when information was written to the disk. With the advent of multitasking systems and the need for larger, faster network operating systems it became the custom to maintain the FAT or its equivalent in memory reducing the number of disk writes by half and greatly increasing the overall speed of the system. This is why it is necessary to go through the shut down procedure on your Windows 95 or Windows NT system.

The problem here is that if a system crashes, it cannot simply be restarted immediately and take up where it left off. The "FAT" must be rebuilt. Most modern operating systems have means of storing the data locations within the data itself so that the table can be relatively easily rebuilt. Unfortunately during this process, the system is down. No critical information can be reported to the operator during this period. If there are extensive files on multiple disks which need to be searched, the process of rebuilding the "FAT" can be a very time consuming process.

To be sure there have been major advances in operating systems which in other ways have greatly improved their reliability. An excellent example is the realtime kernels used in Unix and NT which prevent higher level programs from accessing the processor functions directly thereby greatly reducing the opportunity for system crashes caused by application programs.

Nonetheless as systems grow larger and the market's demand for more user friendly systems increases, so do the complexity of our systems and the opportunity for failure.

IV Mission Critical System Design

To some extent mission criticality is in the eye of the user. To the information systems manager it is the need to protect the files under all circumstances. To the security manager the data files are indeed critical, but even more important is the immediate reporting of critical events. Security information is time critical. You can't take any action until you know an incident has occurred. If the file server or CPU is down, you don't know what is happening. In order to determine the best system design for you begin with an analysis of your needs and a system risk assessment.

1 What is the primary purpose of your system?
  a Will it be monitored all the time?
  b Are there life safety issues involved?

2 How big is your system now and how large might it get?
  a. How many user stations will you need?
  b Will you be on your own network?

3 What type of alarms will you monitor with your system?

4 How many doors will you control? What kind of control do you need?

5 What other functions will the system serve?

6 How will you use the data stored by your system? i.e.: How important is it?

In even the simplest system timely information is usually the most important issue. Here the criteria are clear.

1 The system should use distributed processing so that if one component fails the entire system doesn't fail.

2 The CPU should be dedicated to the security function so that other operations cannot compromise the systems reporting and logging capability.

3 Use a reliable operating system which is not prone to unpredictable failures. Windows 3.x is not a good candidate. Windows 95 can also be a poor choice.

Larger systems offer more complex problems. Clearly the most important criterion is the timely reporting of critical events followed closely by reliable logging and secure databases. If the system is to have multiple workstations as is the case with most large systems, a client server LAN/WAN is the most likely approach. Many design criteria need to be considered for such a system. Only some of the most important can be discussed here.

1 Hardware and System considerations (Figure 4)

  a. Whenever possible use a separate server and LAN for your security system. It is obviously critical that you control when the server is operational and who has access to it. Although both Windows NT and NetWare have excellent security protection which can be augmented by third party hardware, if it is not your hardware, and it is used by others at the same time, they must necessarily have some say in its operation and maintenance. In other words if enough people want it turned off, it will be turned off.

b There should be redundant means of receiving critical information. This can take several forms:

i Redundant Servers, one operating as a hot backup for the other. Unfortunately Windows NT does not support a hot backup. Manual intervention is required to promote a backup server to be primary server. There is third party software available which claims to provide this capability. Both NetWare 4.1 and the RISK version of UNIX do support a hot backup. For this reason alone, NetWare is the preferred NOS for PC based security management systems.

ii In some system designs as a backup procedure in case of server failure, the Local Area Controllers (LAC) can be automatically accessed by a work station forming a peer to peer network. In other designs, a work station can talk to each of the LAC simultaneously logging information and reporting critical events to the operator.

c Redundant Subsystems: In many cases it is simply too expensive to use redundant servers. In these cases subsystems which might fail are often set up in a redundant configuration. One of the more common subsystems for which redundancy is provided is the hard drive(s). Frequently a redundant array of inexpensive disk drives (RAID) is used. In this case data is written to a pair of drives simultaneously. If one of the drives fails, it can be replaced while the system is operating and then data from the remaining drive is transferred to the new drive so that redundancy is restored.

Redundant routers and bridges may also be required, particularly if the entire information pathway passes through one unit.

d Redundant communication paths are nearly as important as redundant servers. A redundant communication path should have no points in common except the LAC and the Server. In both cases the communications ports should obviously be different. Examples of secondary communications paths include the following:

i A secondary copper or fiber line.
ii An RF link
iii A cellular telephone

In the latter two cases encryption should be considered.

2. Operating System Considerations

Some of the best mission critical operating systems for PC s are known only to the most ardent software experts and hobbyists. For better or for worse, the current market wisdom says that Microsoft is the only company which is going to still be around in five years, so if you don't want your investment to be obsolete, base it on a Microsoft operating system. Yet Microsoft does not make a mission critical multitasking operating system. It doesn't even make an operating system which will support a hot backup. To further complicate the matter, the marketplace demands a standard graphical user interface and that standard is Windows.

Industry rumors have it that Windows NT is slowly moving toward a UNIX like architecture which will provide hot backup capability. The NT kernel is already mission critical and the system is preemptive. But what is the solution now.

The most effective PC architecture is a NetWare 4.1 redundant server configuration using Windows NT Workstation or Windows 95 as the workstation operating system. The Local Area Controllers should run their own mission critical OS such as a POSIX compliant UNIX derivative for PCS, a multitasking DOS type system such as DRDOS, CCIDOS or if they are not using multitasking, standard MSDOS. See Figure 5.

The LAC must maintain a copy of the databases which pertain to their functions. They should support redundant communication paths and be able to be re-booted by a watch dog circuit. Communications between the servers and the LAC must be secure. There should be no way for a workstation to communicate to a LAC if it is not specifically designed and set up to do so.

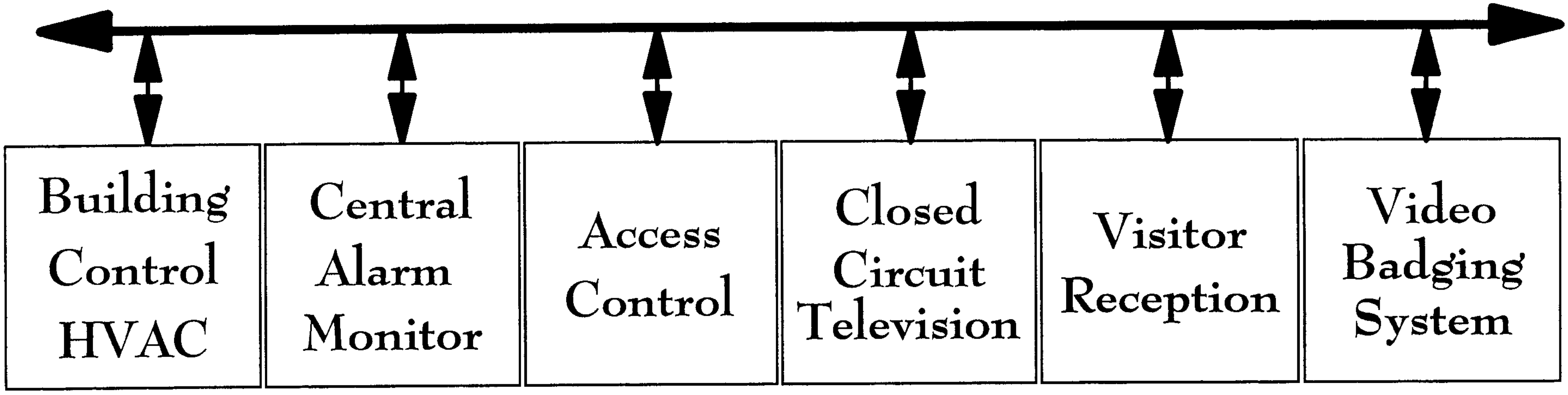
VI, Summary

Early security management systems could be designed to be mission critical. The programming was done in a language close to the processor, so the software could be designed to be highly fault tolerant. But each manufacturer's system was different with no common architecture, and no expansion capability to include other related functions which were not explicitly incorporated by the manufacturer. Improvements in PC operating systems led to a "standard" graphical user interface and a more common architecture. However, as a result of the changes in operating system design which led to these features, it was not possible for the system manufacturers to maintain open architecture and mission criticality simultaneously. Program engineers were forced to write code which did not directly interact with the processor. Now they were dependent upon the behavior of the operating system which lay between their code and the processor itself.

Mission critical systems today require a hybrid approach to system design. If the server system is to utilize a hot backup, it must either use a version of Novell NetWare, or combination Windows NT 4 and third party software. The workstations will utilize either Windows 95, or Windows NT Workstation. The Local Area Controllers will maintain their own databases as well as transmit them to the server. They will support redundant communication links to a server and utilize a mission critical operating system which in general does not support a GUI.

The future will most likely see the evolution of mission critical operating systems for servers. Windows NT is already moving in this direction as is Novell. It is too early to determine whether or not Novell will withstand the Microsoft onslaught.

Modern Security Management System



Features	*Benefits*
Open Architecture	Works with multiple vendors systems The end user can select the best System for each function
PC Based	Easily Serviced, Easy to use, Inexpensive Extensive Software Available
Unified Database	Maximum report generation ability

Figure 1

Fixed Partition Memory Map

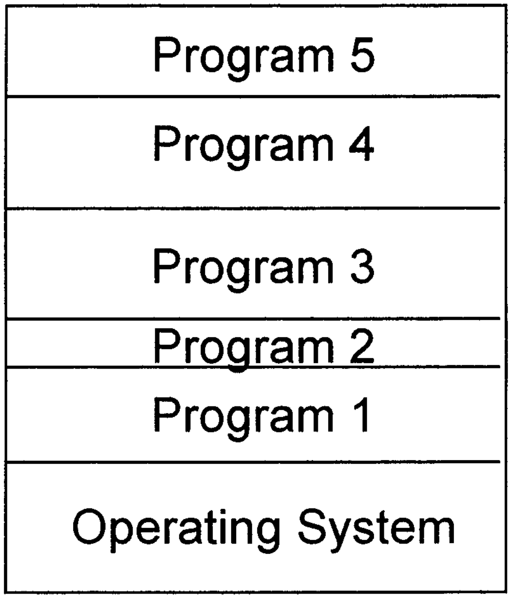


Figure 2a

Dynamic Partition Memory Map

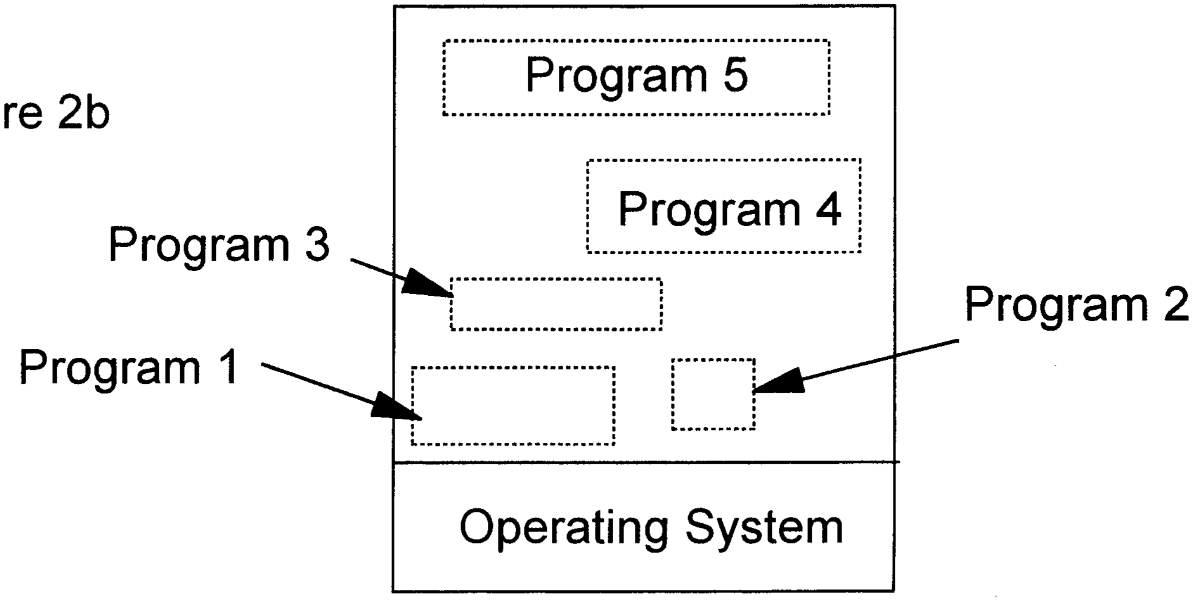
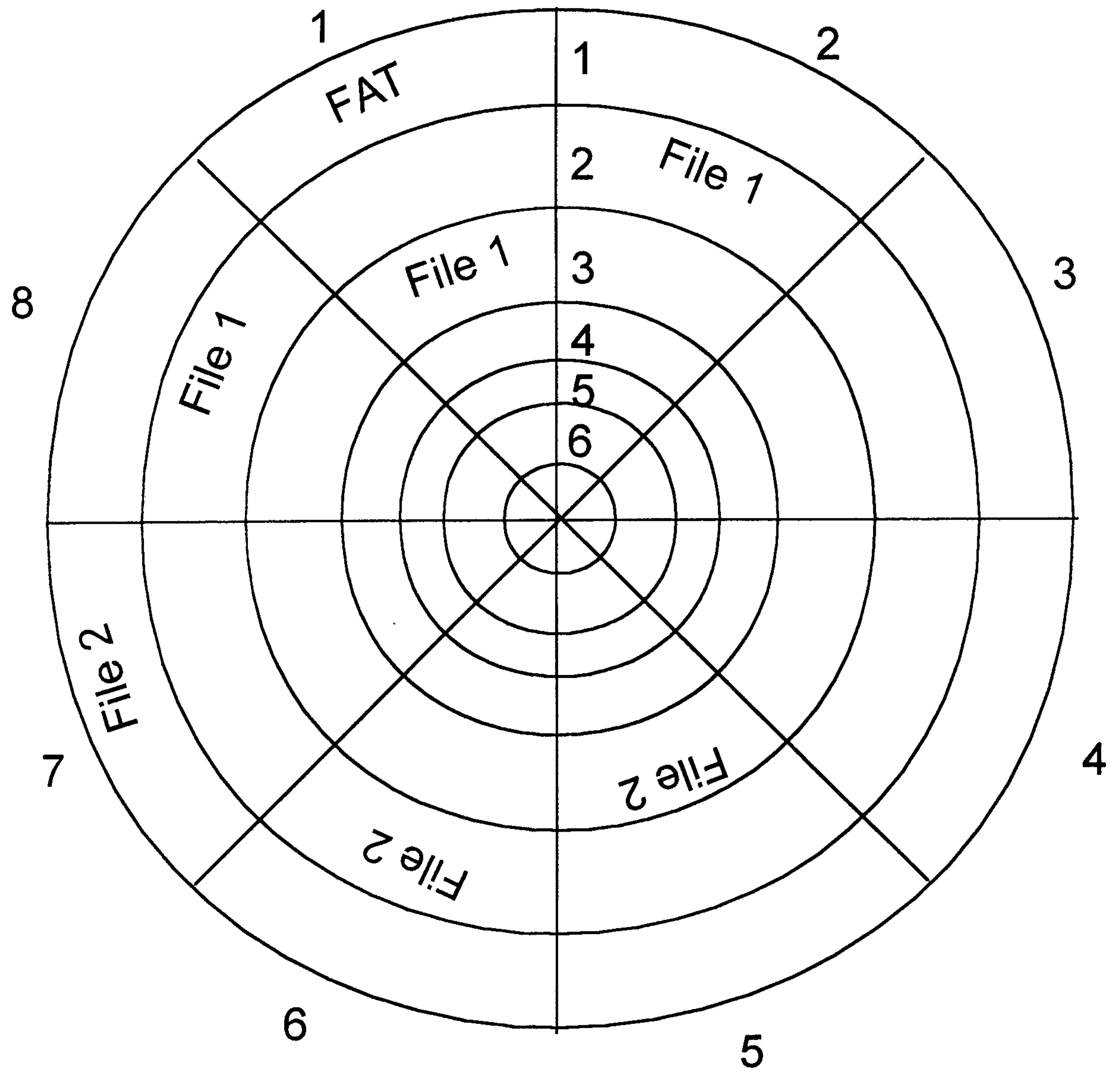


Figure 2b

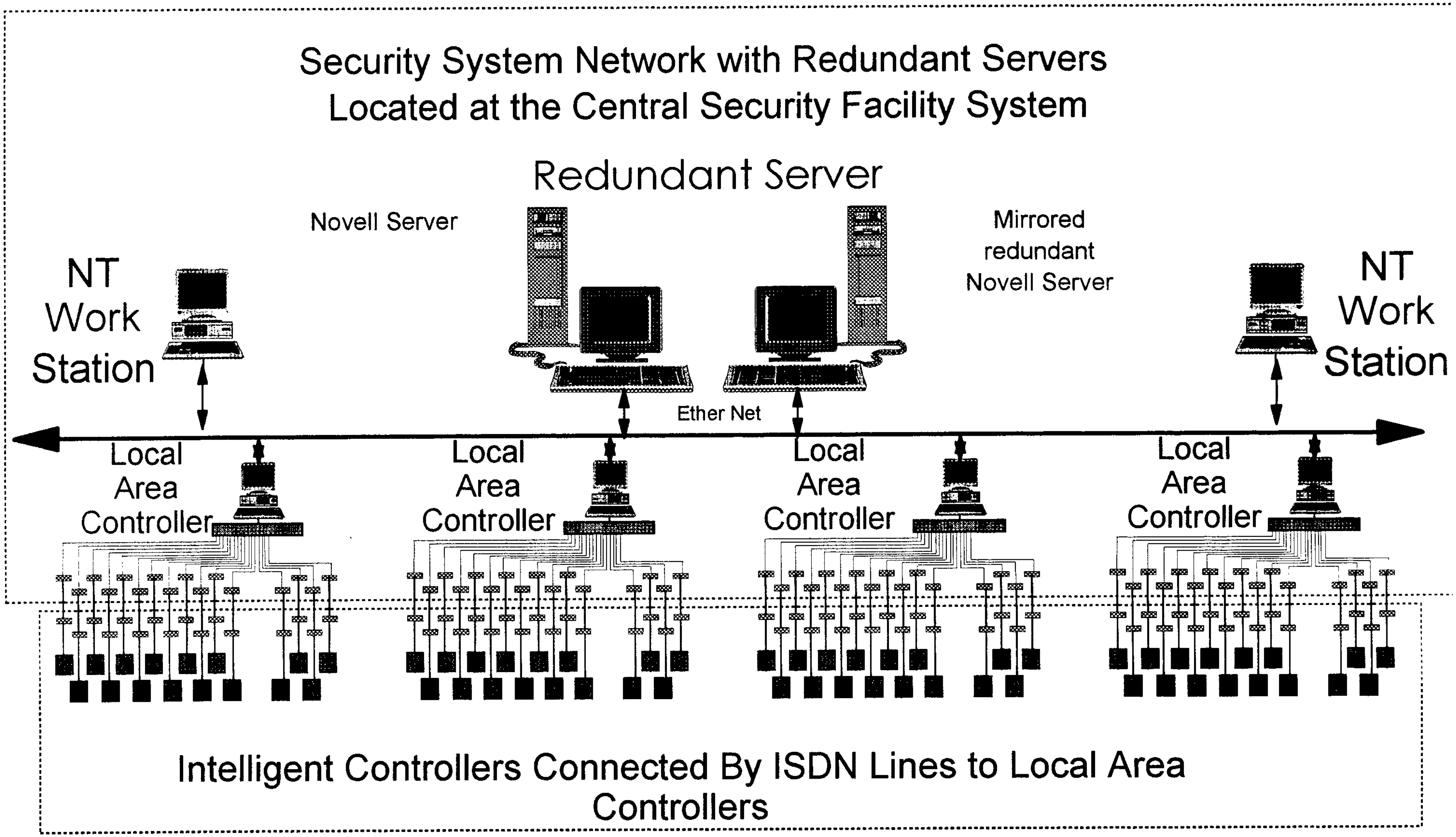
Physical Disk Data Distribution



File Allocation Table

File	Sector	Cylinder
1	8	2
	1	3
	2	2
2	5	3
	6	2
	7	1

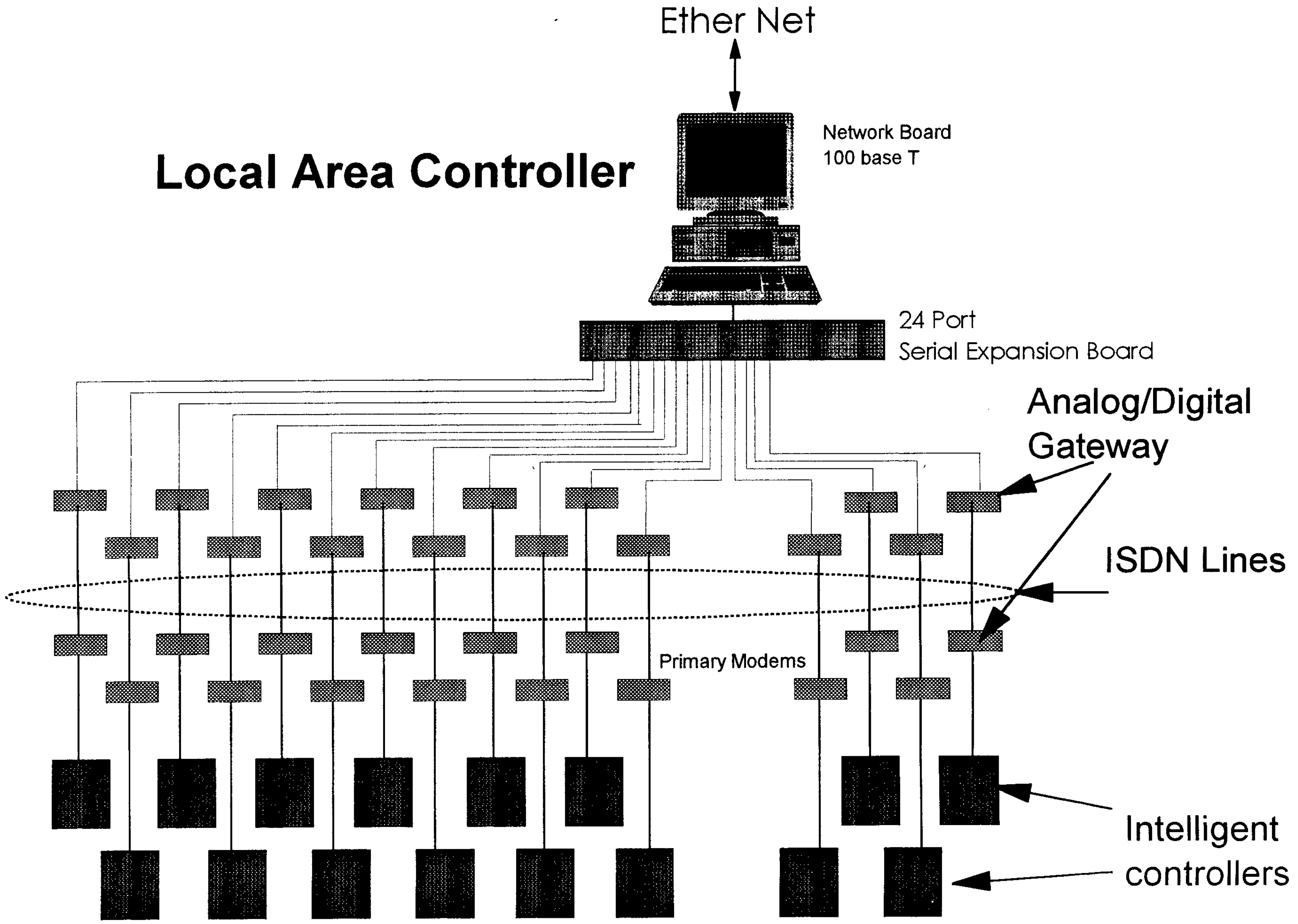
Figure 3



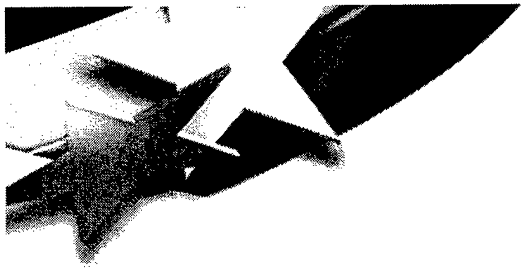
Mission Critical Security Management System

Figure 4

Local Area Controller



Local Area Controller
Figure 5



Risk Analysis Tools for Force Protection and Infrastructure/Asset Protection

Tuesday, June 16, 1998

Session IV: Technical and Policy Focus

Calvin D. Jaeger, Ruth A Duggan and William K. Paulus
Security Systems and Technology Center
Sandia National Laboratories, MS 0759
Albuquerque, New Mexico 87185
505-844-4986, 505-844-0011(fax)
cdjaege@sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy under contract DE-AC04-94AL85000.

Sandia National Laboratories

The Risk Equation

Probability of Attack
Intelligence Agencies
History

Probability of Adversary Success

Consequences
Agency Direction

$$\underset{\text{System Risk}}{R} = P_A \times \overbrace{[1 - \underbrace{P_E}_{P_I \quad P_N}]} \times C$$

Probability of Interruption
Quantitative Analysis Tools
System Testing

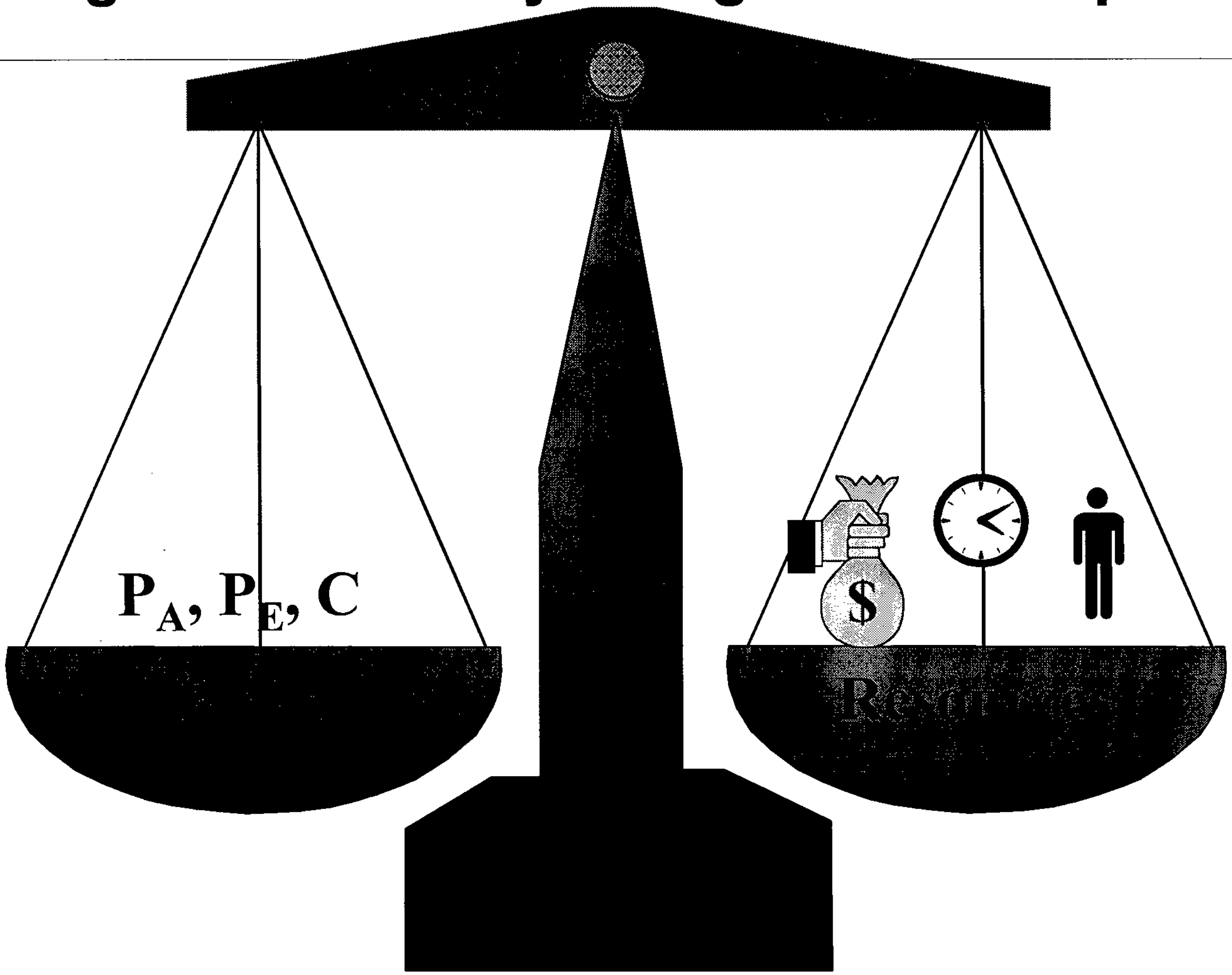
Probability of Neutralization
Force Engagement Models
Response Force Tests

There are no second chances!

Sandia National Laboratories

Risk Management Through EnSURE

Engineered Surety Using the Risk Equation

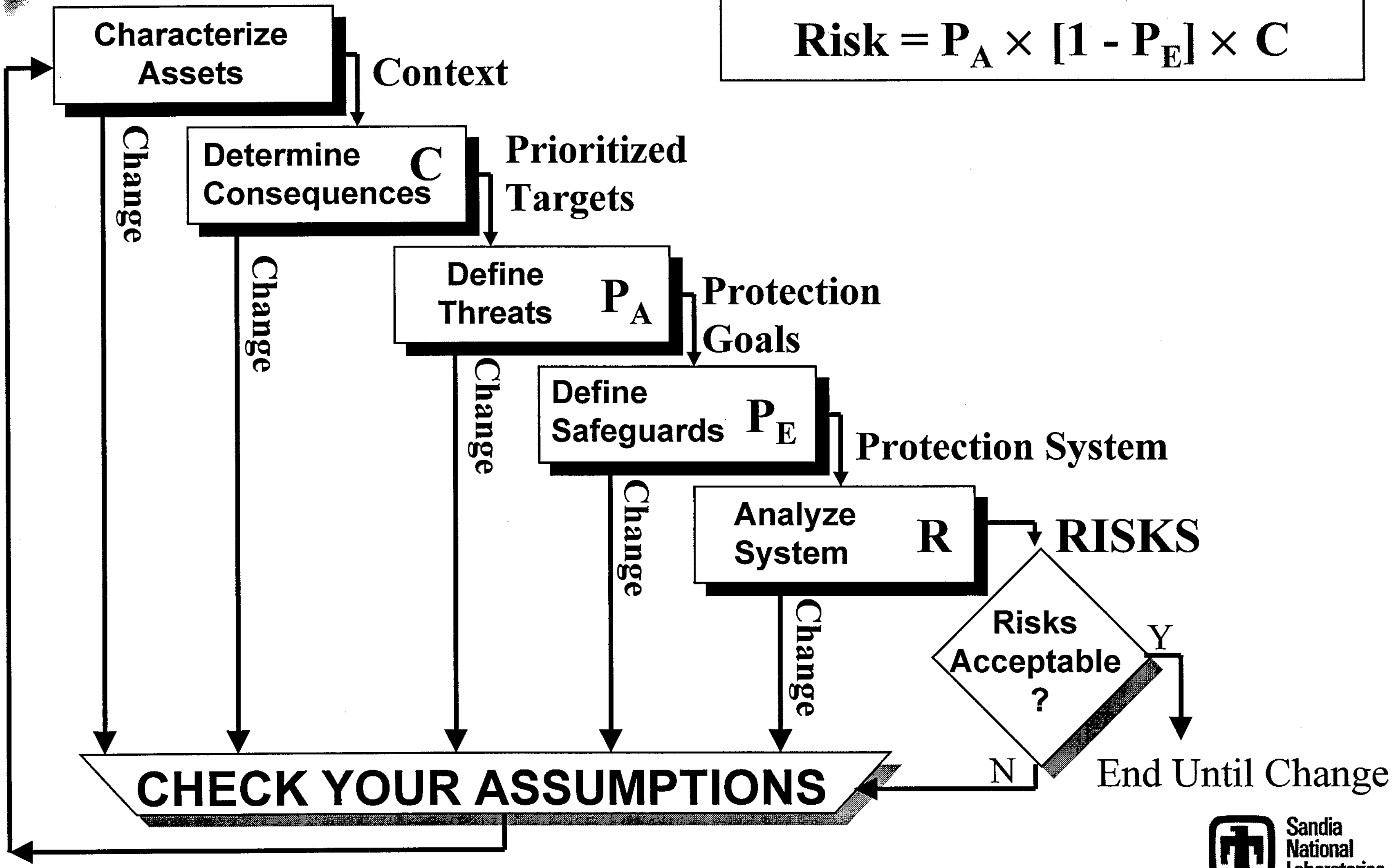


A Process Supported by Tools

Sandia National Laboratories

The Process

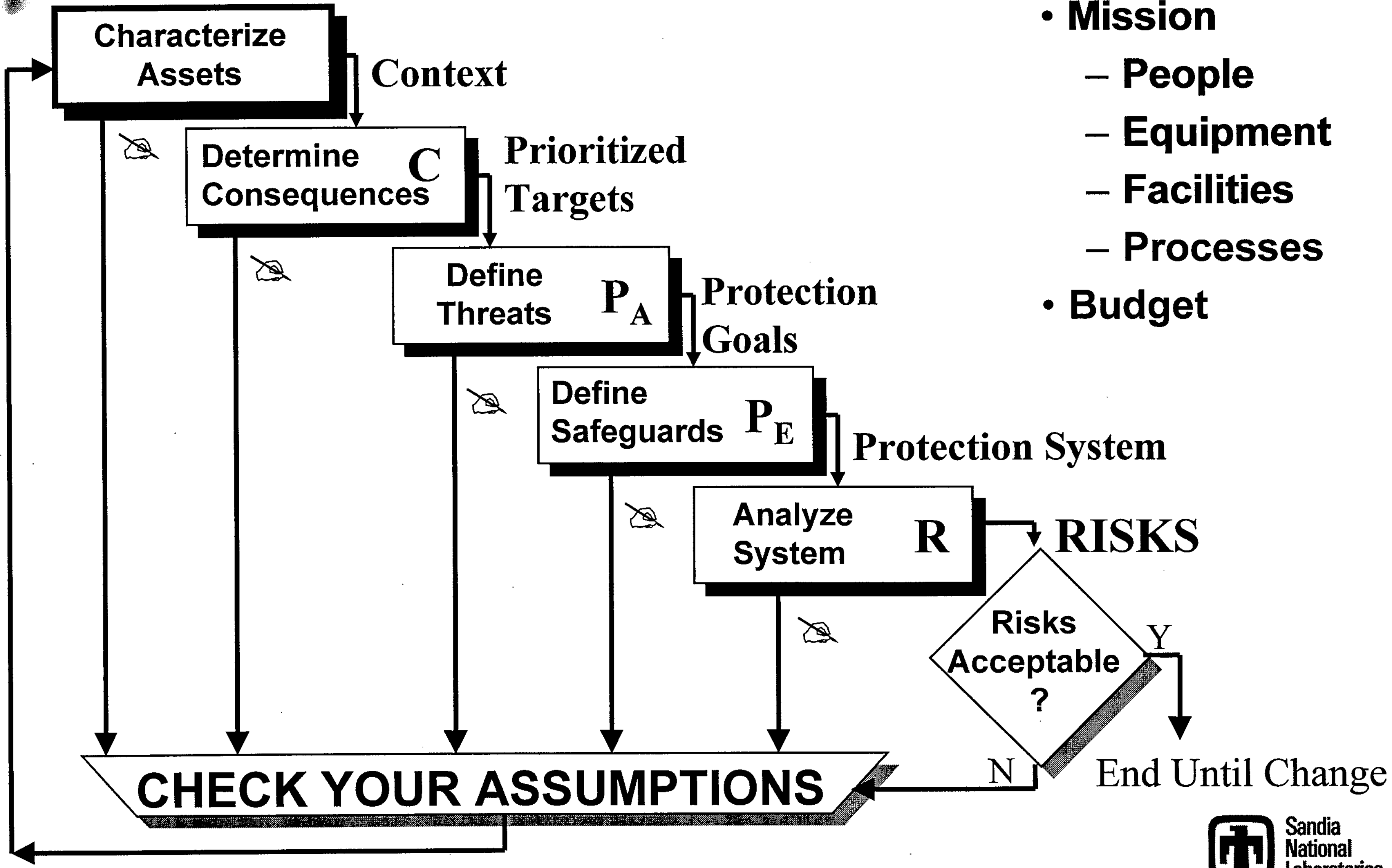
$$\text{Risk} = P_A \times [1 - P_E] \times C$$



Sandia National Laboratories

Characterize Assets

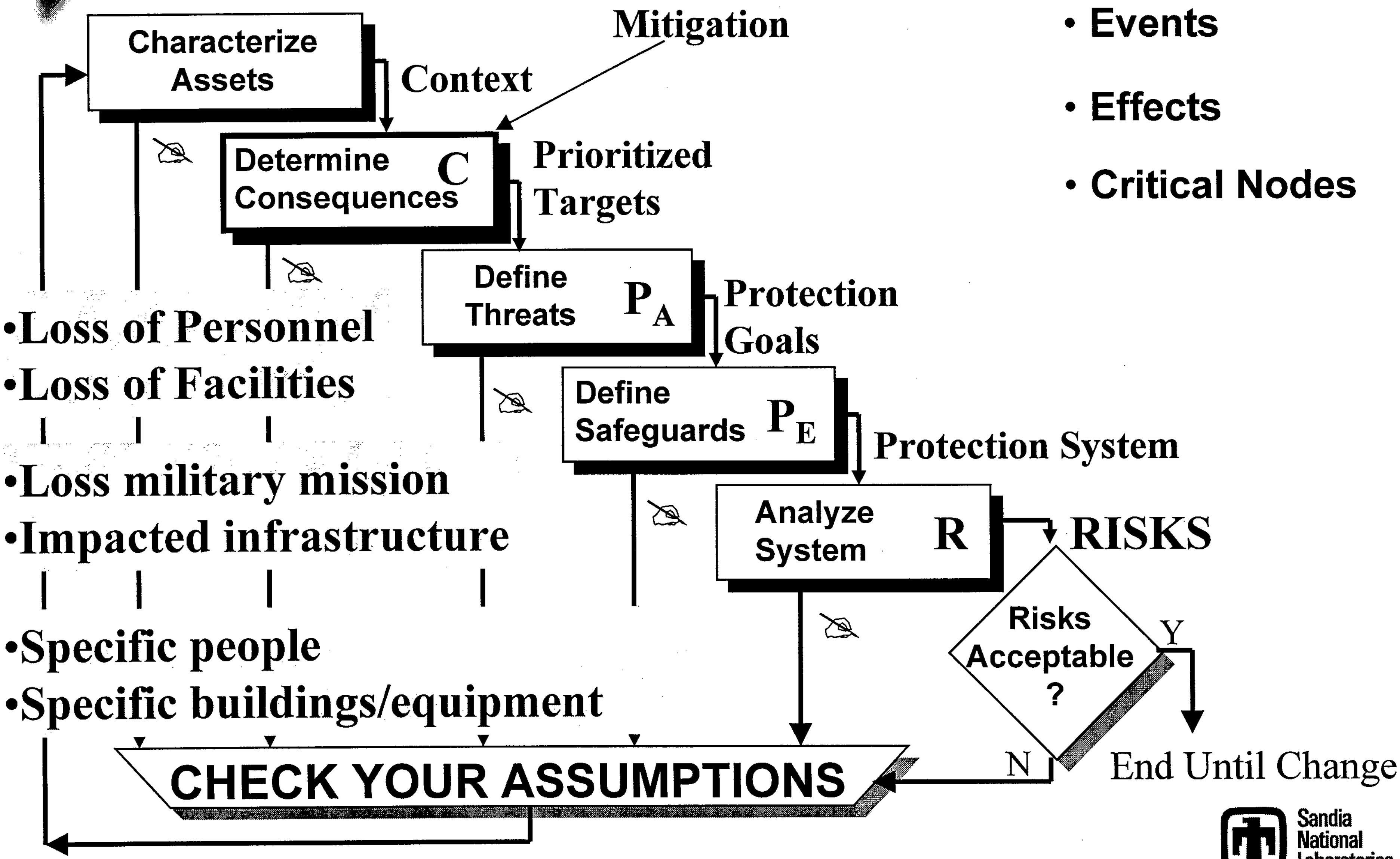
- Mission
  - People
  - Equipment
  - Facilities
  - Processes
- Budget



Sandia National Laboratories

Determine Consequences

- Events
- Effects
- Critical Nodes



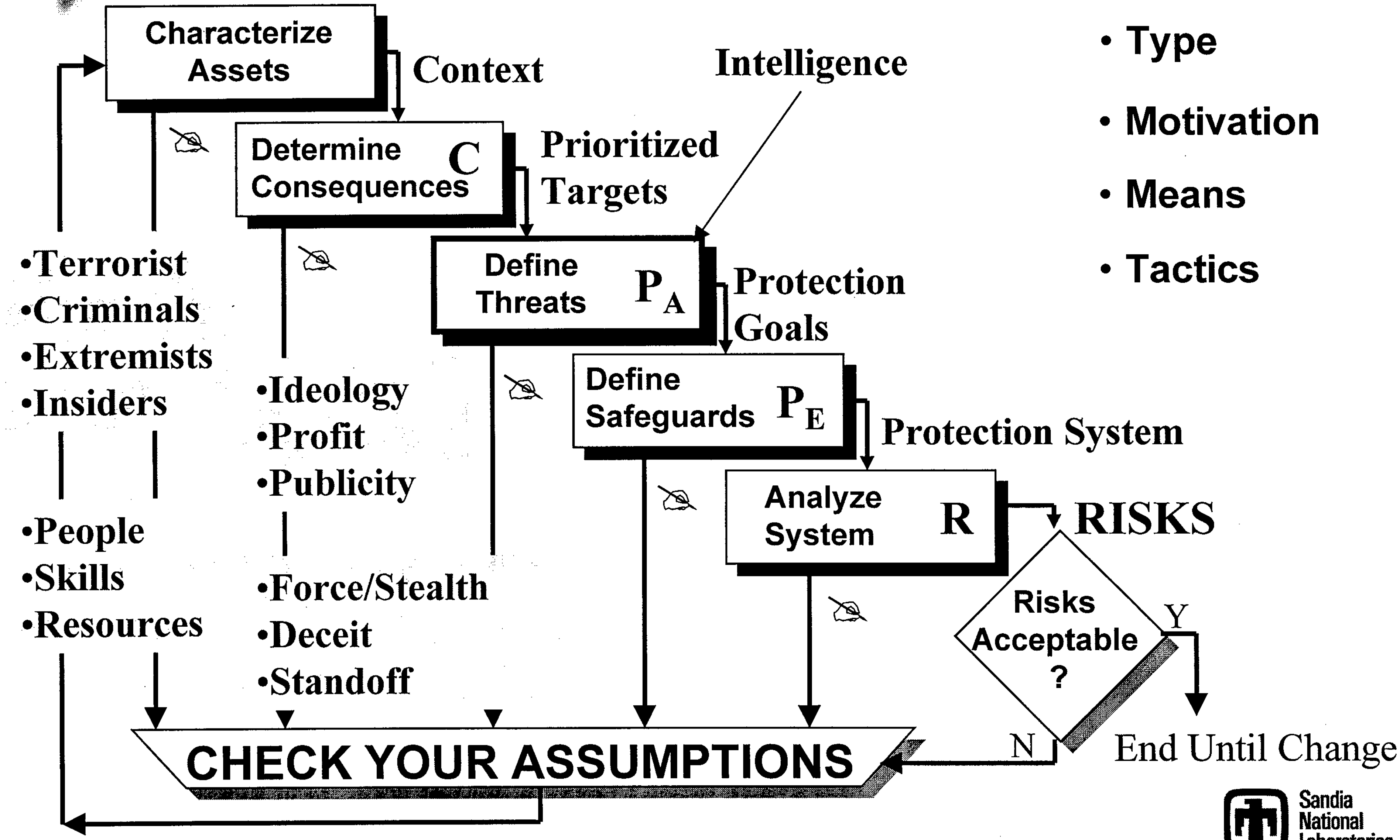
•Loss of Personnel
•Loss of Facilities

•Loss military mission
•Impacted infrastructure

•Specific people
•Specific buildings/equipment

Sandia National Laboratories

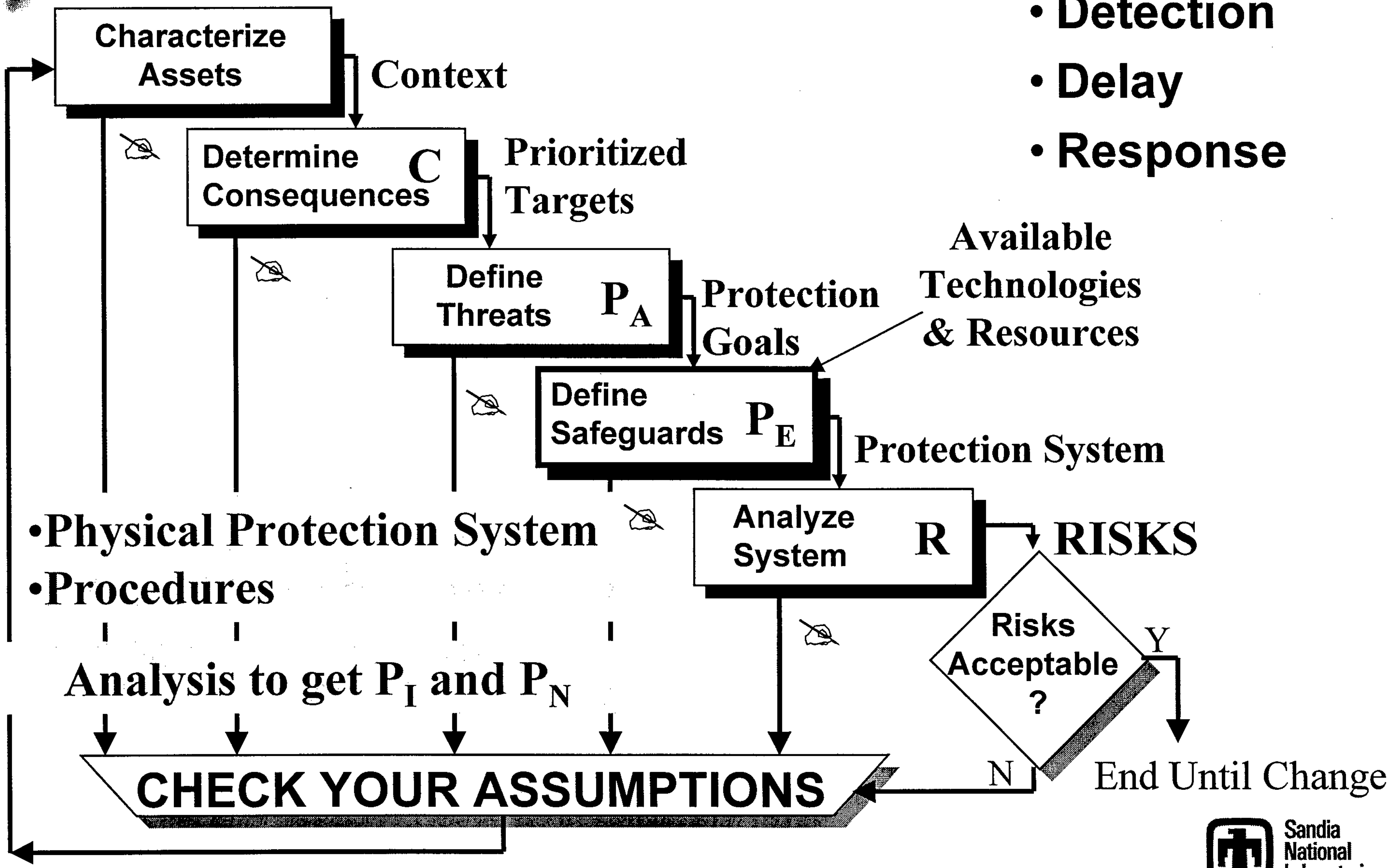
Define Threats



Sandia National Laboratories

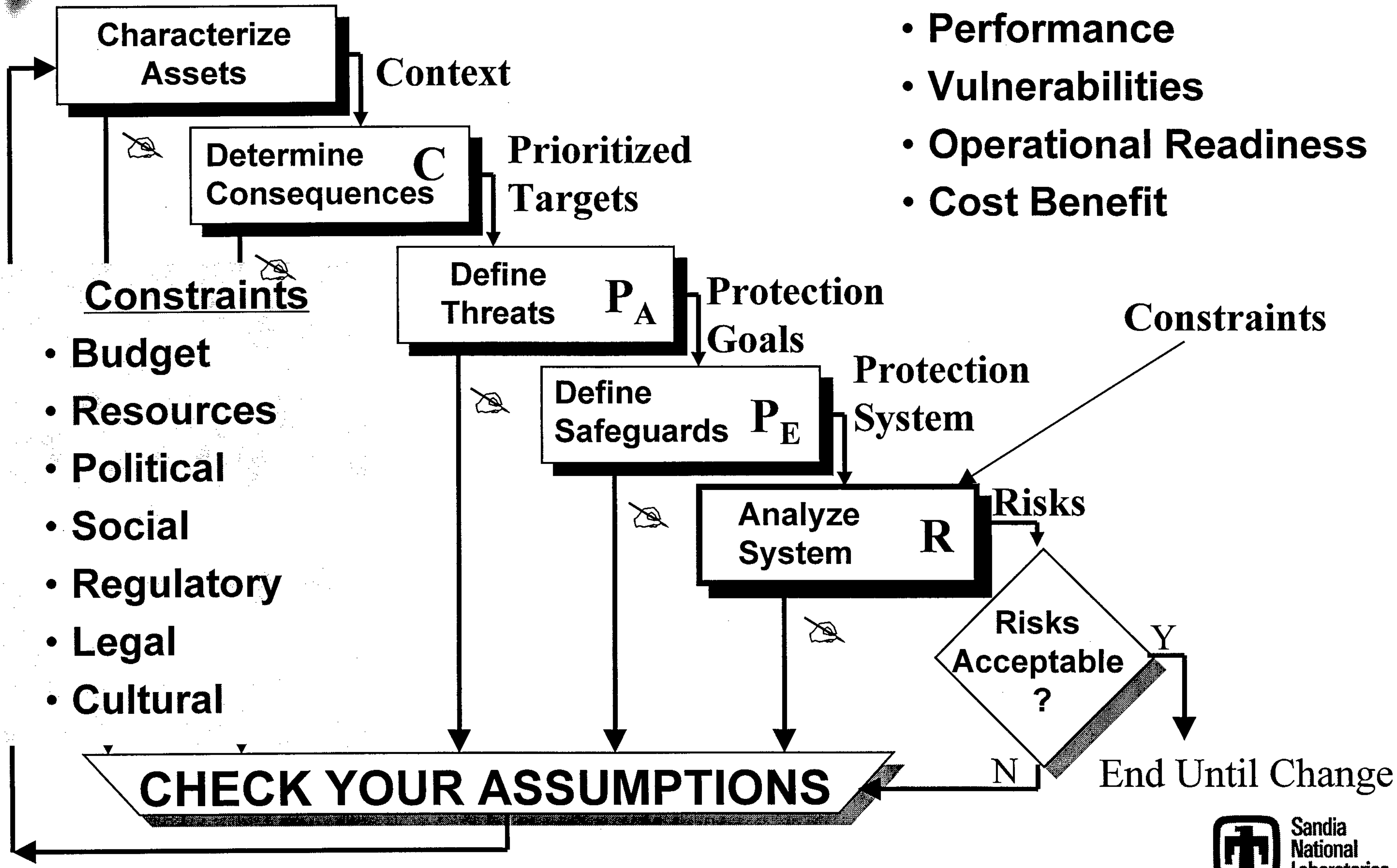
Define Safeguards

- Detection
- Delay
- Response



Sandia National Laboratories

Analyze the System



Characterize Assets

Context

Determine Consequences C

Prioritized Targets

Define Threats P_A

Protection Goals

Define Safeguards P_E

Protection System

Analyze System R

Constraints

Risks

Risks Acceptable ?

Y

End Until Change

N

CHECK YOUR ASSUMPTIONS

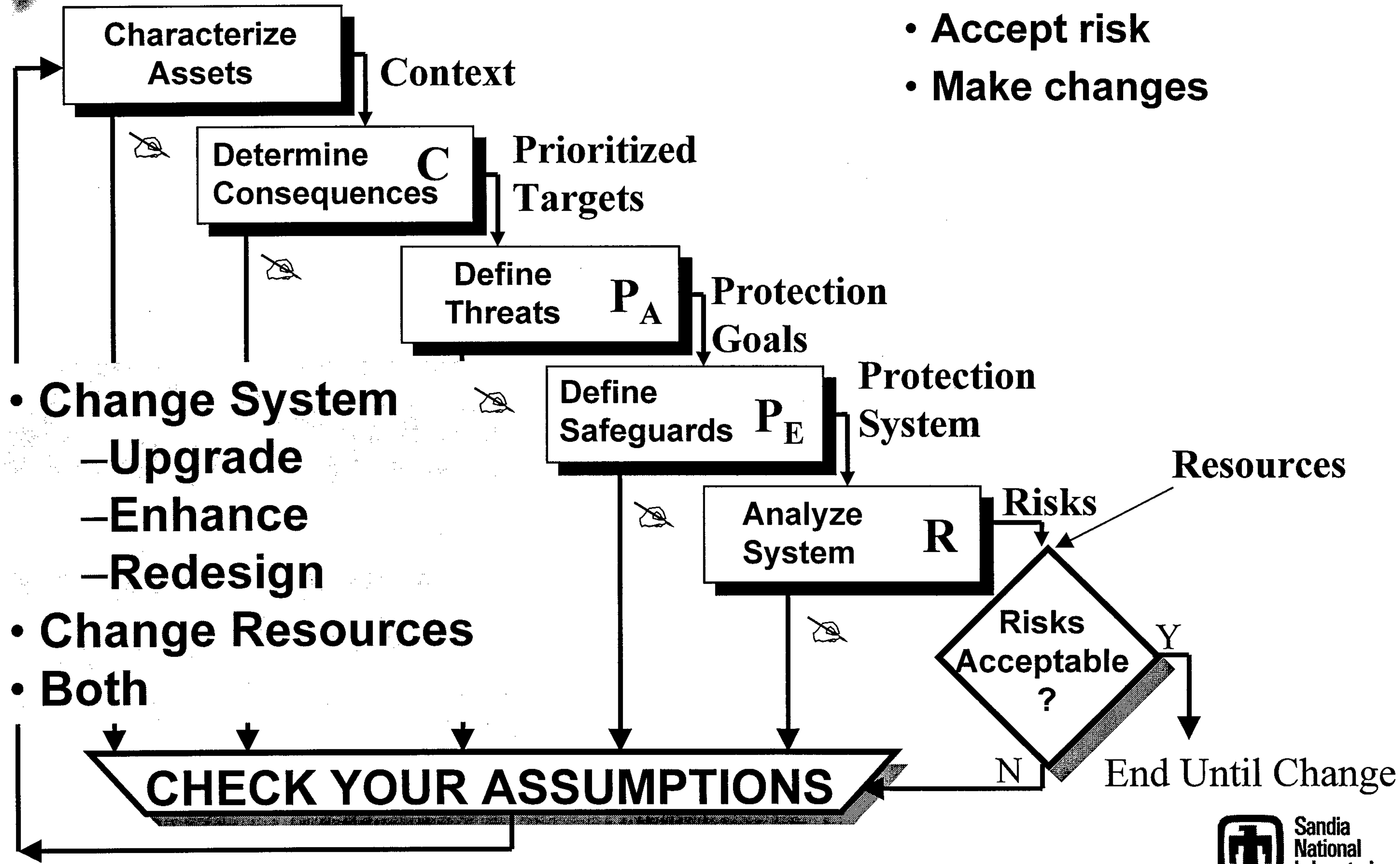
Constraints

- Budget
- Resources
- Political
- Social
- Regulatory
- Legal
- Cultural

- Performance
- Vulnerabilities
- Operational Readiness
- Cost Benefit

Sandia National Laboratories

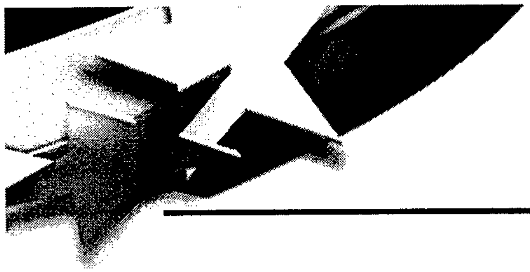
Make the Decision



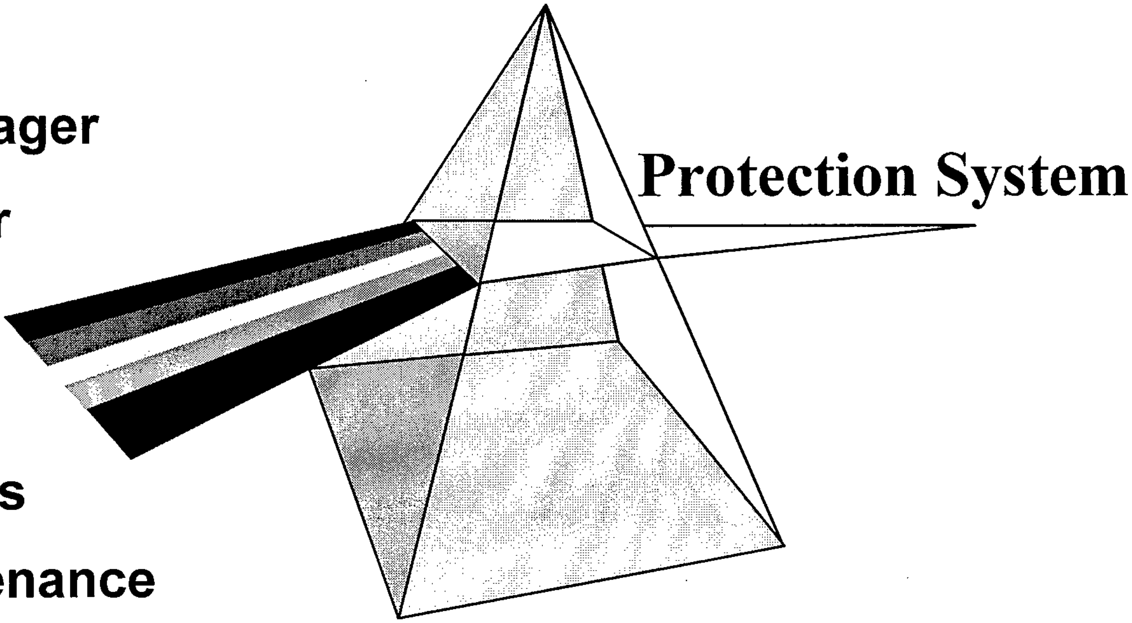
- Accept risk
- Make changes

- Change System
  - –Upgrade
  - –Enhance
  - –Redesign
- Change Resources
- Both

Sandia National Laboratories



Viewpoints



Site Manager

Security Manager

Security Forces

Acquisition

Operations

Maintenance

Protection System

Sandia National Laboratories

Tools

Component	Status
• Characterize the Asset	◒
• Determine the Consequences	◒
• Define the Threats	○
• Define Safeguards	◒
• Analyze System	◒
• Make the Decision	◒

EnSURE

"Complete the Suite"

- Tools
- Interfaces
- Application Guidance
- Decision Support

Sandia National Laboratories

A Management Friendly Transportation SECURITY RISK MANAGEMENT (SRM) Process

By

Lennart E. Long, Security Systems Programs Manager, The Volpe Center

Executive Summary

A Management Friendly Transportation Security Risk Management Process

The National Defense Industrial Association has been working on a quantitative Security Risk Management Process since 1990. David McFadden, the Facilities Security Working Group's Chair has adopted and further developed this Process within the Federal Aviation Administration's FAA Security Division to assess the risk of government assets in terms of dollars for use by the FAA. The FAA team has utilized and further refined this process and is training the FAA Lines of Business in its use and its results. This is being done in order to determine the acceptability of risk of FAA facilities and to rationally and economically meet the requirement of the Presidential Memorandum calling for upgraded security at federal facilities and the Department of Justice Report calling for minimum levels of security at federal facilities.

For more information about this Security Risk Management Process, please call Mr. David C. McFadden at (202) 366-0985 or Mr. Lennart E. Long at (617) 494-2251.

Introduction

SRM Requirement

- Presidential Memorandum requires federal facilities to upgrade security
- The requirement for SRM by all Federal agencies is an integral part of the National Performance Review (NPR).
- The Department of Justice report establishes base -line security requirements for reducing vulnerabilities.

Pure Risk Defined

- Pure risk, unlike business and speculative risk, assumes that a threat will be successful.

- This quantifiable damage is referred to as a "loss event".

- The pure risks in every program, project, operation, system, and facility, must be identified as part of the program conceptual design and planning.

Pure Risk

- Some pure risks must be addressed immediately because of their severity and potential for catastrophic impact on the program.

- Other pure risks of a lesser order may be Controlled.

- Others may be accepted by management.

SRM Objective

- The objective of the SRM program is to ensure that the risks from all types of threats, including risks from criminal and terrorist attacks, are reduced to an acceptable level through the application of cost effective countermeasures.

What is SRM?

- SRM is the logical process that is used to determine:
  - What risks are acceptable
  - What risks are unacceptable
  - What type and extent of countermeasures are required

- SRM is a dynamic and interactive process.

- SRM must be part of the life cycle of every program, project, operation, system, and facility.

SRM Purpose

- To evaluate the risk to the facility in terms of its critical assets
- To quantify risk and establish what risks are unacceptable
- To determine what measures and costs are required to reduce unacceptable risks to an acceptable level

----

SRM Scope

- SRM must be p[art of all Program Implementation plans, funding profiles, and Mission Needs Statements
- The SRM program must be part of the acquisition life cycle from the Mission Needs to the procurement and throughout the effective operational life of the asset.

SRM Goals

- Provide cost effective risk reduction

- Accept some risk, and ensure that prudent security measures are used in all facilities

----

Concept of Asset

- Assets are anything of value to the NAS mission including equipment, personnel, equipment, and procedures
- Each asset has pure risk
- To evaluate pure risk, assets must be quantified in terms of dollars

----

SRM Asset Identification

- Identification of Assets
    - Specific Assets need to be addressed
    - Each asset is evaluated in terms of its:
        - Value in dollars

•Replacement cost

•The impact of dollars that would result from the loss or damage of an asset

SRM Determine Criticality

•Once the asset is identified and quantified, a determination must be made regarding its criticality.

•Criticality is quantified in terms of impact of loss in dollars if the asset is damaged or destroyed.

•Assigning a criticality rating permits prioritization of assets

•Assign a criticality rating by arranging assets in order of priority with the most critical first and the least critical last.

•Criticality Designator 1 – Catastrophic

•Total Destruction or Loss of the asset or sufficiently severe damage to the asset causing complete loss of mission capability for an extended period

----

Criticality Designator 2 – Very Serious

•Major damage top the asset requiring extensive repairs with consequent severe impairment of the mission capability

•--

•Criticality Designator 3 – Moderately Serious

•Damage of the asset is sufficient to require immediate repairs with noticeable impact of the capability of the facility to accomplish its mission

----

•Criticality Designator 4 – Not Serious

•Damage to the asset is such that there is no noticeable adverse impact on the capability of the facility to perform its mission

•------------------------------

•SRM Threat Considerations

•

•Determine what threats are associated with each asset

- •Evaluate all known threats
- •The threat evaluation shall include information from prior risk assessments if available
- •Information from intelligence agencies

•SRM Existing Countermeasures

•Current and planned countermeasures are identified and quantified as to their effectiveness in reducing risk

•----------------------------------

•SRM Determine Vulnerability

•

•Identify and quantify vulnerabilities for all assets

•-------------------------------------

•

•Vulnerability Rating A – Certain

•Given no changes, the loss event will occur.

•-----------------------------------

Vulnerability Rating B – High Probability

•The loss event is much more likely to occur.

•-----------------------------------

•Vulnerability Rating C – Moderately Probable

•The loss event is more likely to occur

•-----------------------------------

•Vulnerability Rating D – Improbable

•The loss event is not likely to occur

•-----------------------------------

•SRM Risk Logic

•Determine the Risk Level by combining

•Criticality Designator (1-4) and

•Vulnerability Rating (A-D)

•-----------------------------------

•SRM Risk Logic – Impact of Loss

•See Process Chart below

•------------------------------

•SRM Risk Logic

•Determine acceptability of risk by interpretation of Impact of Loss data

•-------------------------------

•Risk Logic – Risk Management Guide

•See Process Chart below

•---------------------------------

•Develop Countermeasures

•Evaluate all risk reduction measures for reducing unacceptable risks to acceptable levels

•-----------------------------------

•Perform Cost/Benefit Analysis

•Cost benefit analysis results are arranged in priority order according to their effectiveness

- •Assemble data
- •Review forcing functions
- •Review benefits
- •Review costs for alternate countermeasures

- Estimate percentage of risk reduction for each countermeasure
- Calculate value of benefit
- Calculate cost/benefit ratio
- Compare
- Select or reject

•Repeat until acceptable upgrades are identified

•--------------------------------

•Proceed with upgrade

•The most cost-effective countermeasures are recommended to management in the SRM Assessment Report

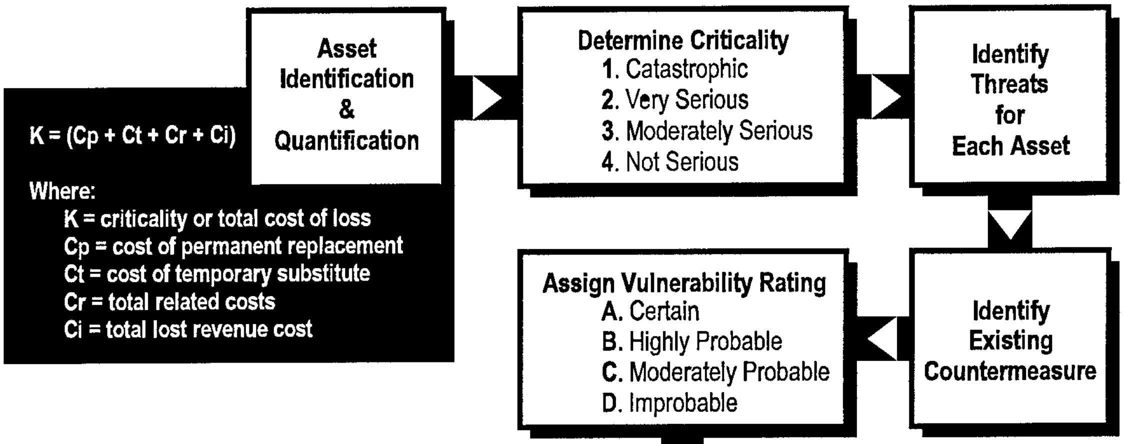
•

•

Summary

- Through the SRM process, resources and funds are concentrated on the most critical assets, and on the risks that pose the greatest danger to mission and people.

FAA SECURITY RISK MANAGEMENT PROCESS



K = (Cp + Ct + Cr + Ci)

Where:
K = criticality or total cost of loss
Cp = cost of permanent replacement
Ct = cost of temporary substitute
Cr = total related costs
Ci = total lost revenue cost

Asset Identification & Quantification

Determine Criticality
1. Catastrophic
2. Very Serious
3. Moderately Serious
4. Not Serious

Identify Threats for Each Asset

Identify Existing Countermeasure

Assign Vulnerability Rating
A. Certain
B. Highly Probable
C. Moderately Probable
D. Improbable

DETERMINE RISK LEVEL

		Impact of Loss			
Assessed Rating	Probability of Loss	1 Catastrophic	2 Very Serious	3 Moderately Serious	4 Not Serious
A	Certain	1A	2A	3A	4A
B	Highly Probable	1B	2B	3B	4B
C	Moderately Probable	1C	2C	3C	4C
D	Improbable	1D	2D	3D	4D

DETERMINE ACCEPTABILITY OF RISK

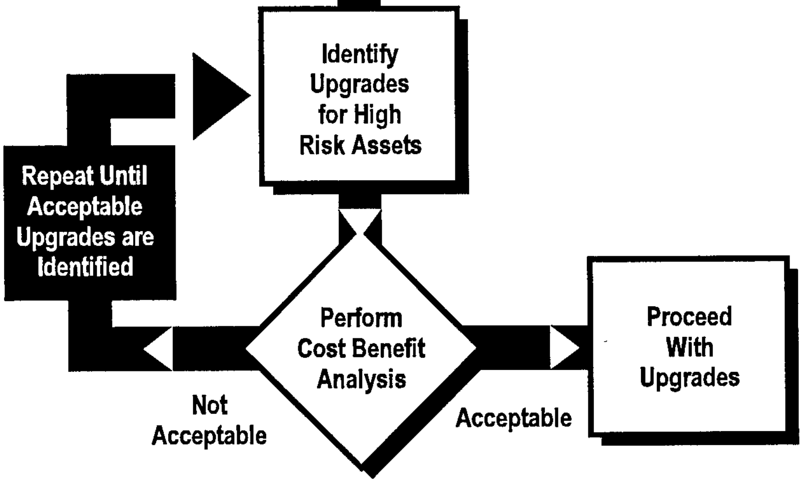
FAA Asset Risk Level	Interpretation
1A, 1B, 1C, 2A, 2B, 3A	These risks are unacceptable and must be controlled or eliminated.
1D, 2C, 2D, 3B, 3C	These risks should be unacceptable. However, management may determine to accept the risk in writing.
3D, 4A, 4B, 4C, 4D	These risks may be accepted with management review.

PURPOSE

I. To evaluate the risk to the facility in terms of its critical assets

II. To quantify risk and establish what risks are unacceptable

III. To determine what measures and costs are required to reduce unacceptable risks to an acceptable level



Identify Upgrades for High Risk Assets

Perform Cost Benefit Analysis

Not Acceptable

Repeat Until Acceptable Upgrades are Identified

Acceptable

Proceed With Upgrades

End of Presentation

This presentation is the product of the Volpe Center. The sponsor of this product is the Federal Aviation Administration.

For more information, contact:
Lennart E. Long
617-494-2251

Airport Vulnerability Assessment – An Analytical Approach

NDIA Security Technology Symposium
Williamsburg, VA, June 15-18, 1998

Author: Rick Lazarick, FAA Technical Center, Aviation Security R&D

ABSTRACT

The Airport Vulnerability Assessment Project (AVAP), which is currently in progress, is the direct result of congressional funding of recommendation 3.13 of the White House Commission on Aviation Safety and Security. This project takes a new approach to the assessment of US commercial airports. AVAP uses automation, analytical methods and tools to evaluate vulnerability and risk, and to analyze cost/benefits in a more quantitative manner.

This paper addresses both the Process used to conduct this program as well as an unclassified look at the Results which have been achieved for the initial airport assessments.

The Process description covers the acquisition approach, the project structure, and a review of the various methodologies and tools being used by the 8 individual performing organizations (Battelle, BDM, SAIC, Lockwood Greene, CTI, Abacus Technology, Science and Engineering Associates, and the Naval Facilities Engineering Service Center). The tools described include ASSESS, SAM, RiskWatch, CASRAP and BlastFX. Included in the process is the establishment and use of an advisory panel made up predominantly of experts from the National Laboratories (Sandia, Oak Ridge, Argonne and Brookhaven).

The Results portion addresses the findings and products resulting from the initial airport assessments. High level (unrestricted) summaries of the results are presented, along with initial trends in commonly recommended security improvements (countermeasures). Emphasis is placed on positive noteworthy findings, showcasing the approach taken by airports with particularly good security practices. A summary of significant Lessons Learned is provided.

To conclude this paper, a project status and anticipated schedule for the next year is presented.

Introduction

The Federal Aviation Administration (FAA) sponsored Airport Vulnerability Assessment Project is the direct result of Congressional funding of recommendation 3.13 of the White House Commission on Aviation Safety and Security. Initiated in April 1997, this project is now just over one year old and significant progress has been achieved. This paper addresses the first round of airport assessments that will be completed in FY 98. What makes this project significantly different from all of the previous airport assessments is that it takes a new approach to the assessment of US commercial airports, using automated, analytical methods and tools to evaluate vulnerability, risk and cost/benefits in a more quantitative manner.

The following sections of this paper will trace the progression of the project from its inception to its current status. First is a description of the procurement process used to expedite the contracting of these vulnerability assessments and a summary of the technical approaches being employed. Next is a discussion of some generalized results of the assessments that have been completed. Finally, the plans for continuing this project are provided.

The Airport Vulnerability Assessment Process

To establish the project requirements and to assure that the assessments are conducted with a common threat definition, the FAA developed a detailed statement of work (sow) which established the minimum requirements for all performing organizations in terms of tasks and deliverables. Additionally, a set of 16 unique threat scenarios were established by the FAA. These generic threat scenarios defined the target (e.g. passenger aircraft), the threatening act (e.g. bombing), the aggressor (e.g. terrorist) with characteristics (e.g. originating passenger, non-suicidal), and the contraband (e.g. improvised explosive device, in luggage). These generic threat scenarios were then used by the contractors at each airport, and modified as required to fit the characteristics of that site. The FAA solicited all Category X and I airports looking for volunteer airports to participate in this effort. In all, 29 airports offered to participate.

One of the distinguishing characteristics of this AVAP is the acquisition strategy employed. The FAA, taking advantage of the acquisition reform policies recently afforded to the agency, used a combination of directed procurements and competitive awards to achieve contract arrangements with 8 different performing organizations in a period of only five months. In addition, the statement of work included a novel approach, in that a minimum requirement was established for airport vulnerability assessment. However, the contractors were encouraged to add to this minimum, any aspects of airport assessment which they felt would satisfy the needs of the airport security planners, such as risk assessment, cost-benefit analysis and cost-effectiveness of proposed countermeasures. Since the contracts were to be let as fixed priced contracts, the degree of additional analysis effort (beyond the minimum requirements of the SOW) was described in the technical proposals, and price was not used as critical evaluation criteria.

The objective was to obtain a wide range of vulnerability assessment approaches, utilizing several different quantitative methods and various automated tools. The clearly stated theme of this acquisition was "Do It Your Way", meaning that the FAA spells out the fundamental aspects of the effort (What needs to be done), and the contractor is completely free to establish the methodology for the assessment (How it will be done). This approach, as you will see, resulted in a wide range of methods and tools.

Six airports were assigned to three performers based upon the FAA's knowledge of their vulnerability assessment experience via a non-competitive directed procurement and a Military Interdepartmental Purchase Request (MIPR). (see table of performing organizations and assigned airports).

The competitive procurement process was used to contract five additional performing organizations. Initially, a Screening Information Request (SIR) was issued, and twelve organizations responded with corporate capability and experience statements. Upon FAA review, six of these were selected to receive the request for proposal (RFP), and a bidders conference was conducted. Formal technical and price proposals were submitted, and upon review by the FAA, five of the bids were awarded contracts for 1 or 2 airport assessments. From SIR announcement to contract award, this streamlined acquisition process took a mere 15 weeks.

ORGANIZATION	ASSIGNED AIRPORT
Abacus Technology Inc.	Denver (DEN)
	Detroit (DTW)
Battelle	Cincinnati (CVG)
	Louisville (SDF)
	Salt Lake City (SLC)
BDM Federal	Atlanta (ATL)
	Boston (BOS)
Counter Technology Inc.	San Juan (SJU)
Lockwood Greene Technology	Colorado Springs (COS)
Naval Facilities Engineering Service Center	Seattle-Tacoma (SEA)
	San Francisco (SFO)
SAIC	Miami (MIA)
	Jacksonville (JAX)
Science & Engineering Associates	Orlando (MCO)
	Newark (EWR)

Methodologies

The intent of the acquisition process was to obtain contractor services which represented a wide range of technical approaches to airport vulnerability assessment. As a group, the contractors' approaches do represent a highly diverse set of assessment techniques, each of them proven in previous facility vulnerability assessment efforts primarily for the DOE, DOD and some public access facilities. The challenge now is to evaluate how well each of these techniques can be applied to US domestic airports. The following paragraphs briefly outline the basic approach and any automated tools being used by each of the contractors in this assessment.

Abacus Technology Inc.

The Abacus Team approach uses a combination of quantitative and qualitative analyses. The quantitative approach is supported by the use of the Security Assessment Model (SAM) originally developed for the NFESC. It is a detailed facility assessment tool with emphasis on detection opportunities, delay timing, response force timing and interdiction success. This tool strictly assesses facility vulnerability. In addition, Abacus is using the commercial product RiskWatch to assess the overall airport facility. RiskWatch includes vulnerability assessment, identification of potential countermeasures, risk analysis and cost-benefit analysis. Limited testing is included in the Abacus approach.

Battelle

The Battelle Team uses two complimentary techniques in their analysis. First is a manual technique known as the Analytical Risk Management (ARM) process originally developed by the CIA. ARM is a threat, vulnerability and risk assessment process that relies heavily on the expert opinions of the assessment team members. Additionally, the Civil Aviation Security Risk Analysis Process (CASRAP) developed by Akela for the FAA was used to assess the airport as a whole, and to validate the ARM methodology. CASRAP is based on an earlier product, SASSY, with a specific focus on US airport characteristics. It also includes vulnerability, risk and cost-benefit analyses. Very little testing is included in the Battelle approach.

BDM Federal

The BDM team includes RiskWatch, Inc., the developers of the tool "RiskWatch", which is the primary focus of their assessment method. RiskWatch addresses the analysis of vulnerability, risk and cost-benefits for the candidate countermeasures. RiskWatch is a commercial product, which was previously adapted to be specific to US airports. For scenarios involving the analysis of explosive blast effects, BDM uses the BlastFX model, which they developed under contract to the FAA. The model estimated building structural damage as well as the extent of human injury. The BDM approach does not depend upon testing, but does involve extensive questionnaires for the airport and air carrier employees to complete.

Counter Technology Inc. (CTI)

CTI uses both a quantitative and a qualitative approach to airport assessment. The quantitative approach uses a scenario flow chart depicting alternate aggressor path and the detection opportunities along those paths. Tabulated data is then used to evaluate the detection probability considering all of the possible mitigating circumstances. CTI is currently automating this process, utilizing hypertext links to facilitate information interconnections. Additionally, CTI is utilizing the CARVER methodology, which is a more qualitative, target selection process, with increased focus on airport overall risk assessment. Testing is used to validate the findings.

Lockwood Greene Technology

The Lockwood Greene Team is performing a quantitative analysis using a technique known as AVAT (Advanced Vulnerability Assessment Technique). AVAT is a derivative of the ASSESS model developed for use by the DOE, and utilizes portions of the ASSESS databases. The implementation is more of a spreadsheet style form, organized by layers, with detection, assessment, delay and response values. Further, an Adversary Intercept Diagram is developed to analyze response force actions. Testing is used to validate inputs to the assessment technique.

Naval Facilities Engineering Service Center (NFESC)

DOD experience is applied to the airport assessment project by the Risk Analysis Vulnerability Assessment (RAVA) Team from the NFESC. The RAVA methodology is largely a manual process, using expert judgement and structured questionnaires to quantify the airport vulnerability and risks. Supplemental information is provided by utilizing automated tools for explosive blast effects, and the Security Assessment Model (SAM). The RAVA Team makes extensive use of testing to verify the perceived vulnerabilities. These tests are highly structured, well coordinated, video recorded and are non-disruptive to airport operations or passengers.

Science Applications International Corporation (SAIC)

SAIC uses a “table top” approach which is very simple and straightforward. The Team conducts a normal data gathering phase, and then performs an interactive analysis involving airport security and law enforcement personnel. During this interactive table top session, agreement is reached on qualitative judgements of the security system detection, assessment and response capability. Numbers are applied to these “expert opinions” and calculations of vulnerability and relative risk are provided by an MS Excel spreadsheet. Countermeasure sets are then assessed as to their effect on risk, and costs to implement are estimated. SAIC does not include testing in their process.

Science & Engineering Associates (SEA)

The SEA team uses a highly quantitative approach involving the use of the tool, Analytical Software System for Evaluation of Security Safeguards (ASSESS). Sandia

National Laboratory, Livermore National Laboratory and SEA originally developed this tool for the assessment of DOE. SEA has begun modification of the code toward an airport oriented version of ASSESS, utilizing portions of the underlying database of security component detection and delay data. SEA depends upon testing to verify timing information and unique detection situations. The SEA Team conducts tests to verify vulnerabilities determined by preliminary analysis. The testing process is highly structured and non-intrusive.

Blue Ribbon Panel

The intent of the project was to conduct airport vulnerability assessments, and as a by-product to examine the processes used by various contractors and to determine the "best practices". To advise the FAA and to assist in the evaluation process, a Blue Ribbon Panel (BRP) was established with security professionals not involved in the assessments. The panel has members from the US Army Corps of Engineers and the National Laboratories (Argonne, Brookhaven, Oak Ridge and Sandia). A highly structured evaluation process is being applied to the evaluation of the contractors' plans and analysis reports. Also, feedback is obtained from the airport recipients of the reports and the FAA agents involved in the assessments. The feedback indicates, from the end-user's point of view, the value, quality and usefulness of the contractor's products and processes. The BRP is tasked to recommend a method to proceed with for future FAA sponsored airport vulnerability assessments. Further, the BRP is tasked to examine the available automated tools demonstrated in these assessments, and to recommend to the FAA a roadmap for proceeding to a tool (or set of tools) which are suitable to use in the field.

Airport Assessment Results

As would be expected, the results of the widely varied methodologies, applied to a set of diverse airports, are anything but identical. It is not the purpose of this paper to divulge specific findings for named airports. However, there are interesting trends and inconsistencies which are noteworthy and these can be discussed with airport anonymity.

Compliance

One of the general findings which is uniform is that the airports studied are predominantly in compliance with the FAA regulatory requirements. The Threat Scenarios prepared for this analysis were known to probe into area which are not highly regulated, but which are plausible terrorist approaches. Therefore, some of the scenarios result in relatively high calculated levels of vulnerability, and, for the most part, the highest vulnerabilities are logically predictable.

SIDA

Airports utilize a personnel identification security feature known as the Security Identification Display Area (SIDA). Each airport defines the SIDA in their Airport Security Plan, and it includes the security sensitive areas of the airport operations, such as the ramp area immediately surrounding parked aircraft. In this area, all personnel are required to display their ID badge (above the waist on their outermost garment). Furthermore, all employees are trained in SIDA practices, and are required to challenge any person in the SIDA area without a displayed badge.

The degree to which the SIDA practices are adhered to and enforced varies drastically among airports. Some approach the issue by providing incentives, such as small cash awards, for properly challenging a test subject. Many airports have the authority to issue "tickets" to anyone found not to challenge an unbadged person. Some of the punitive methods are so harsh that they are rarely enforced, which renders them useless. The best examples appear to be sites that combine active incentive programs with moderate (but enforces) punishments. But the dominant characteristic that is present at airports with good SIDA challenge practices is a high level of employee security awareness, the source of which is elusive.

Screening Point Staffing

Even prior to this study, it was a well-established fact that the screeners who man the airport checkpoints are subject to very high turnover rates. This can be explained in large part to the very low wage scale (minimum wage), the stress associated with the security responsibility of the screener, and the lack of job satisfaction (boredom, abuse by the public). There are many emerging technologies that will directly effect the screeners. New and more complex detection equipment may require a higher or different level of screener perception and training. Threat image projection systems should increase screener vigilance, improve detection of more types of threat objects, and provide a means of measuring screener proficiency. Screening point equipment improvements can only be effective if used by capable screeners.

Perimeter

Most airports have perimeter fences or natural barriers which are intended to impede an intruder from entry into the Air Operations Area (AOA). Analyses of threat scenarios that involve perimeter incursions indicate that the perimeter barriers provide only a small degree of delay to the intruder. Once inside the AOA, an intruder may have unimpeded access to aircraft or secured portions of the airport facilities, with varying degrees of potential detection by roving police patrols and/or employees who may of may not challenge intruders. Those airports that have installed Perimeter Intrusion Detection Systems and have adequate lighting and CCTV surveillance capabilities are much less vulnerable in these scenarios.

Access Control

Most airports have access control systems that control doors and/or gates from the public side of the airport to the secure side. Frequently, the personnel ID card is also used as the access control media. In some airports, the access control system has characteristics that greatly improve the security posture. For guarded gate control, the access control system can provide to the guard, a picture of the badge-holder for identity verification. For controlled doors, upon alarm the system can immediately display the camera image associated with that door (and is some cases, a "history" of that camera signal at or just before the alarm time) to the person responsible for assessing the alarms and initiating law enforcement dispatch.

Law Enforcement Staffing

Generally, the law enforcement practices observed at the airports were very professional with well-documented procedures. The ability to respond to threatening events at the screening points in a timely manner was generally adequate. One consistent shortfall however is the ability for timely response to other airport locations and the frequency of roving patrols. This is a direct result of the level of staffing that is established for the airport.

Countermeasures

The range of potential countermeasures identified by the contractors is as wide and varied as the approaches being used. However, the following list is representative of frequently mentioned security improvements. In many cases the airport specific cost-benefit analysis will dictate the appropriateness of the specific countermeasure.

Security awareness and training
- Screener training
- SIDA Challenge awareness for all badged employees

Policy and Procedures
- Background checks (more extensive, periodic updates)
- Positive Passenger Baggage Matching
- Employee screening
- Pre-flight aircraft inspections
- Random screening – checked baggage, cargo

Equipment
- Upgrade screening point equipment
- Perimeter intrusion detection systems
- Improved lighting and surveillance
- Enhanced CCTV (digital recording, exterior coverage, alarm linkage)

Lessons Learned

The foremost lesson learned from the execution of this project is the effectiveness of detailed, comprehensive and timely coordination. The potential exists for significant disruption of airport and air carrier personnel activities in the process of gathering the information necessary to carry out the extensive analysis to be performed. However, through the advanced acquisition of key documentation, introductory coordination briefings, and the designation of an FAA lead at each site for coordination, this project has achieved a minimal level of disruption.

Testing activities have also generated several lessons. Coordination of test plans with all effected parties is essential. In some cases, it is also essential to keep the test subjects unaware of the test to keep the results unbiased. Coordination with managers of the staff under test must be accompanied with explicit instructions to keep the test blind. The response of an organization to testing situations must be carefully observed, and unusual staffing arrangements at the time of planned testing is likely to indicate an intent to skew the test results.

Safety is the most important aspect of test planning. In airport testing, no live explosives or functional weapons are ever used. High fidelity explosive simulants have been developed specifically for airport site testing. Dummy detonators and disabled weapons are used and serve the purpose of detectability by the screening equipment without being a safety hazard. Controllers are used extensively to step in at any point of potential conflict between the mock adversary and an airport employee or security person.

Where to from Here?

By the end of this fiscal year, all 15 airport assessment will be completed. The Blue Ribbon Panel will determine the quality/effectiveness of each of the approaches and by December 1998 will have a recommendation to the FAA. The funds appropriated for continued Airport Vulnerability Assessment in FY99 will then be used to proceed with additional assessment performed by the selected contractor(s).

By March 1999, the Blue Ribbon Panel will provide to the FAA a recommendation on how to proceed with automated tools for field use. If one of the existing tools is deemed appropriate, then the FAA could proceed with immediate implementation. If product improvement is called for, the FAA must determine the best manner for bringing the products up to the required capabilities. Ultimately, the FAA plans to have a standardized practice, augmented by automated tools, for assessing airport vulnerability at a local level.

Cost Impact of Residue Sampling And Collection Strategies for Drug and Explosive Residues

By
Joseph J. Fortuna
and
Daniel Lucero

Chemical Detection Services, Inc.
7240 F Telegraph Square Drive
Lorton, VA 22079
Phone: 703 550-1806 Fax: 703 550-1808
Email: chemdet@erols.com

CHEMICAL DETECTION SERVICES, INC.

14TH ANNUAL NDIA SYMPOSIUM & EXHIBITION ON SECURITY TECHNOLOGY

EVENT #849
JUNE 15-18. 1998 WILLIAMSBURG, VA

ABSTRACT

Screening operations for illicit drug or explosives residues comprise two basic processes: 1) sampling and collection of the residue on an appropriate matrix, and 2) analysis of the sample or residue by an analytical device. Commercially available analytical devices require an initial capital investment. The analysis process is not labor intensive. Conversely, the sampling and collection process is a labor intensive process with high consumption of expendables. Two basic sampling and collection methods, with several variations, are employed in the field screening operations: wipe sampling and vacuum sampling. Both methods are preferred over the other for specific screening scenarios. An engineering analysis backed by field screening experience shows that significant cost differences arise with each method. Without trading-off data quality and for identical sampling strategies, a variation of vacuum sampling incurs the least cost by a significant margin over wipe sampling and other vacuum sampling operations.

BACKGROUND

The development of techniques to collect field samples of residues for analysis with today's illicit drug or explosives detectors has been left to the users of these instruments. Manufacturers appeared to focus their attention on the analytical instrument. This has led to very sensitive (sub nanogram for cocaine), fast (5 seconds), and reliable performance (low false positive/false negative rates). The performance of the entire process of sample collection, preparation, introduction, analysis, and interpretation is reduced from the detector performance itself. The sampling strategies (methods and techniques) used to collect residue samples significantly impact the operational cost of the effort. The sampling strategies need to be evaluated in the context of what the user is going to do with the analyses results. In this paper we discuss the merits and shortcomings of various collection techniques and show the cost impacts of each method. We begin by examining two very common sampling scenarios.

SAMPLING SCENARIOS

The paper describes two sampling scenarios which the authors suggest represent two diverse operational constraints. One scenario involves sampling targets where time is not a significant factor. An example of this would be looking for illicit drugs in high school lockers. The number and surface areas of the lockers are large and sampling techniques are dependent on thoroughness (minimizing false negatives) and avoiding cross contamination (a major source of false positives [1}).

The second scenario involves sampling of targets where time is a major constraint. An example of this would be sampling checked luggage for explosives at an airport. The number of pieces of luggage, the variety of surfaces, orientations, and the need to sample and analyze within six seconds (FAA design goal for single luggage) are constraints that shape sampling and analysis strategies.

SAMPLING AND DETECTION OPERATIONS

Sampling operations concerning contraband drugs or explosives are presently limited to hand held collection modules. Automated walk through portals, break cargo, or luggage systems have been under development by the Federal Aviation Administration. The ideal contraband residue collector system would be hand held, battery operated, and very flexible in acquiring residue samples, and analyzing and interpreting the results within seconds. This tool does not exits.

However, the maturation of field chemical residue instruments for illicit drugs and explosives has created the possibility of large scale deployment of detection systems. Yet, this deployment has legged behind expectations. Some of the reasons for this are that the illicit drug contraband interdiction community has experienced false positives at too high a rate to encourage routine use of these systems. The counter terrorism community is more concerned with the potential for false negatives cargo, or luggage systems have been under development by the Federal Aviation Administration. This paper concentrates on hand collection of residue samples. The authors assert that the analysis of the hand held collection process needs to be performed prior to attempting to design and engineer an automated system.

Contraband packages, whose exterior surfaces are contaminated with residues (illicit drugs and explosives) are detectable by the inspection of the exteriors of break cargo and luggage. The search for illicit drug residues in these situation is one of interdiction. The search for explosives residues in these scenarios are for security and interdiction.

There are four other scenarios that one searches for explosives residues [2]:

1. At post-explosion scenes and on items recovered from such scenes
2. On suspects clothing and hands
3. In premises - on work surfaces, tools, shelves, etc.
4. In vehicles - either suspects' vehicles.

Thus sample collection can come from a variety of surface materials which present unique problems to the collector. For example, break cargo and luggage can be leather, cloth, cardboard, plastic, aluminum, etc. The surfaces can be rough or very smooth. The surfaces may be susceptible to marring by abrasion or the action of solvents used in the collection process. The surface can be stationary or moving. The surface may not be readily available to the collector and requires physical contact. The target surface may be located considerable distances from the analyzer. There may be a time constraint, such as with luggage at airports or with perishable commodities at ports of entry.

SAMPLING PROTOCOL CONSTRAINTS

Sampling is the most important and least engineered aspect of the detection process. The engineering process must begin with a solid understanding of the requirements of the user. The collection process may need to be thorough, have no sample cross contamination, and meet the constraints of the sampling scenario (time, location, etc.). The most appropriate sampling tools and protocol are determined by the detection scenario and the detection requirements. Defining these requirements is the first step in the detection operation. The requirements determination process identifies the essential constraints, such as time, manpower, location, time-on-target, etc. In many way cases the user cannot define the requirements adequately. Thus the service provider can best obtain an insight into the requirements from questioning how the user intends to use the information resulting form the analyses.

For the purpose of this analysis we evaluated two scenarios. One, is collecting residue samples from stationary objects (high school lockers) and surfaces for forensics. Two, is collecting from cargo, mail, parcel post, break cargo, or luggage moving on a conveyer for interdiction of contraband.

Each of these sample collection scenarios present unique problems to the collection team. In the case of sampling high school than for false positives.

The goals of Instrument manufacturers is to develop highly sensitive and relatively specific instruments. Manufacturers have incorporated software algorithms that enhance the specificity of the instrument. Yet false positives and negatives associated with sample collection and transport have been ignored. This paper provides an overview of an engineering analysis of the sample collection issues. Sampling techniques, materials, prevention of false positives, and minimizing false negatives are discussed.

The authors suggest three primary operational goals of the sampling collection process:

1. Collect residue of interest
2. Minimize collecting other substances that may mask or cause false positive responses in the instrument
3. Collect and transport residues without loss or contaminating the collector

These goals and how to achieve them are discussed next.

SAMPLE COLLECTION METHODS

There are two basic methods of residue sample collection: wiping and vacuuming. Wipes can be wet or dry. Vacuuming can be with or without contamination control.

Wipe sampling employs some type of collection material that is suitable to the surfaces to be sampled, compatible for transferring the collected sample to the instrument desorber, disposable, and inert to the detector if input directly into the instrument desorber or if a chemical extraction processed is used. Wipes used are Teflon, cloth (typically cotton), and filter paper. Wipes can be used in conjunction with dilute solvents, such as alcohol. The choice of solvents is important since operationally one is concerned with damages target surfaces, with chemical reactions between the solvent and the chemical residues of interest, the temperature effects if direct desorb is used while wipe pad is wet, and concern for exposure effects to humans through contact and through inhalation.

Vacuum sampling employs a collector nozzle, a filter, a filter holder or support, an exit port and a vacuum pump. There are two types of collector nozzles available: controlled and uncontrolled.

A controlled nozzle is one which employs air boundary layers throughout the nozzle to eliminate aspirated particles from striking and sticking to interior surfaces of the nozzle. The boundary layer tends to focus aspirated particles to the filter matrix with out loss. An uncontrolled nozzle will become contaminated with use as particles will strike and adhere to the interior surfaces of the nozzle. With uncontrolled nozzles sample residue is lost. The lost material has two negative affects on the operation. One effect is that false negative results are more likely, since the mass of residue aspirated could be near the lower detection limit of the instrument, and the loss of some or all of this mass could lead to a missed opportunity of detection. The second negative effect is the possible occurrence of false positives from the dislodging of previously collected samples, which were deemed negative but did indeed have residue that was lodged in the nozzle and dislodged by the new sample aspirated particles.

One manufacturer markets a hybrid sampler which employs a vacuum and a wipe strategy to sample surfaces. Upon analyzing this hand held collector, the authors concluded that the collector material used and the vacuum air velocity employed by the module were incompatible and that the device functioned primarily as a wipe mechanism.

Thus the state of collection methods for hand held modules are limited to a four choices, wet wipes, dry wipes, uncontrolled nozzle, or controlled nozzle surfaces. We next examine the techniques and scenarios where residue sample collection is needed.

CRITERIA FOR DETERMINATION SAMPLE COLLECTION METHOD

What is the best way to sample the surfaces of these articles, collect the residue, and transport the collected residue to an analytical instrument, which is usually located in the vicinity of the check point? The answer to this question is important for hand held, manual operations and for the design of automated sample collection schemes. To answer this question a set of criteria needs to be defined in quantitative terms. These criteria are derived from the detection requirement analysis.

This set on criteria is used to evaluate the sample collection options. The criteria list that the authors consider critical are:

- Time: How much time is allowed and needed to collect residue samples?
- Expendables: What expendables items are used and what are the logistics for keeping them readily available?
- Cost: What is the labor cost, expendable items costs, etc.?
- Detection: What is the minimum detection rate of the system?

- False Positives: What false positive rates can be tolerated and at what cost?

- False Negatives: What false negative rates can be tolerated and at what cost?

These criteria have different values the three collection scenarios and for the degree of importance placed on detecting and identifying the residue.

SAMPLING TOOL AND PROTOCOL IMPACTS

Specifications for sampling tools and protocols are a function of operational performance requirements. Sampling and collection technologies employed in residue sampling impact the performance of the analytical detector. The sampling, collection process has taken a back seat during the development of fast, reliable field residue detectors. The collector modules provided by detector manufacturers have severe contamination problems and are not field friendly, They lack engineering. The systems appear to have been developed as an after thought and then primarily for a laboratory environment rather than field sampling.
For example, one manufacturer supplies a hand vacuum that requires the users to assemble the collection filters in a clean environment. The filters are easily damaged once fabricated and are prone to coming apart do to poor assembling. These filters are fine in a laboratory environment where perhaps a handful of sample are run each day, but in the field the contraband screening requires sampling of hundreds of items such as suit cases in very short time spans.

The authors observed the contamination and operational problems while performing field trials with these devices and during hands-on experiments. Cross contamination and collection efficiency were found to be major operational specifications. These and other factors involved in achieving the objectives of sampling are discussed below.

<u>Collecting the particles of interest</u>. Ideally one would desire to collect residues of target materials only. However, this is most unlikely as particles of interest are very likely to be mixed and even adhered to other particles. The need to reduce the contamination of a given sample depends on a number of factors: the amount of target material mass available compared to other materials, the likelihood that contaminating materials could degrade, mask or otherwise invalidate an analysis, the sensitivity of the detection technology to the other collected particles.

The source of extraneous particles could be from dust, pollen, and from the collector matrix itself. The example of the impact of contamination of samples was reported by Revenue Canada [3]. Revenue Canada reported that when using the Barringer Ionscan and wipe sampling documents that signals obtained form cocaine and heroin place on a clean filter were compared to the signals obtained from the targets after the filter was rubbed onto a card which been filled out with inks. The degradation of the signals due to the presence of the ink was observed.

During wipe sampling of packages and mail in prisons also produced indications of procaine from the ink. This was observed by one of the authors in December 1996. The impact of rubbing unwanted chemicals unto a sample matrix may not be critical for situations where false negatives are not crucial to safety and security. But in situations where false negatives are disastrous, such as screening for explosives, the introduction of competing or masking chemicals could be a major problem. Tests such as those performed by Revenue Canada [3] need to be performed, but in the mean time vacuum sampling should minimize this problem.

Vacuum systems, however, to date have been the source of false positives as extreme care by the operator has been necessary to ensure nozzles are contamination free [4]. The dislodgment of contamination residue in subsequent sampling is source of false positives, which the manufactures have left to the operators to resolve via operating procedures. The operators have responded by trying various operationally inefficient procedures and ultimately most operators use wipe sample collection over vacuum sampling.

For any automatic collection process this is a major engineering constraint. Mechanical wipes must be disposable and compatible with the instrument's desorber. Vacuum nozzle's and residue transport segments must be free of contamination. The need for thoroughness in the collection processed must be defined for automated system design.

In situations where forensic analysis is needed, contamination-free vacuum modules would greatly expedite forensic sample analysis. The on-site systems would identify samples on or in which trace particles of explosives were detected, thus reducing the number of exhibits requiring laboratory analysis.

Sampling Thoroughness and Speed. Sampling thoroughness and time to sample are tradeoff parameters. The moving luggage or break cargo scenario requires very fast sampling rates. The FAA has specified that each luggage piece has to be sampled, the sample analyzed, the analysis interpreted in six seconds. Today's fastest of today's detector instrumentation (ion mobility spectrometry) takes five seconds to perform the analysis and interpretation functions. This leaves one second to sample the luggage and transport the sample to the instrument.

SAMPLING OPERATION OBSERVATIONS

Obviously, to meet the six second constraint, not all pieces of luggage on a conveyor can be sampled. Or if they all are to be sampled how can this be achieved? But this raises the question of the pieces selected for sampling how thorough need be the process? Do all surfaces need to be sampled? What percentage of a selected surface need to be sampled?

These basic questions have been left unstudied. The focus has and continues to be on improving the detector/interpretation process and on the characteristics of residues, by not on how the practical methods of collecting and transporting specimens to the detector. The authors have used various counter narcotics and explosives detectors in contraband searches at airports, border crossings, ports of entry, and in the work place. From these experiences we have made the following observations:

1. Drug contraband carrying containers whether from users or smugglers will have relative large quantities of illicit residue on them, thus thorough (100 percent sampling) is not necessary.

2. Explosives contraband containers will have relatively small quantities of residue on the exterior and thorough sampling is required.

3. Residues of interest will be found where people handle the container. For example, handles, zippers, belts, labels, and likely hand holds are the best place to sample. Sampling 100 percent of an article may not be necessary, but the authors do suggest that this area of study begs to be considered. Wipe sampling of specific high residue target areas can be performed very fast and thoroughly.

4. Wipe sampling requires a double transfer of the residue of interest. First the residue has to be collected by the wipe material, than transferred from the wipe material into the instrument detection module.

(The authors have observed that for the ion mobility spectrometers, wipe samples are themselves only partially sampled by the instruments detector module. For example, one cloth wipe has a surface area of 5250 square millimeters (mm). The surface area analyzed by the desorber of the instrument is less than 491 square mm or 9.3 % of the surface area. Users compensate for this in two ways. They try to analyze the most soiled part of the wipe or they try to remember to wipe the pressure point (where their finger was).

5. Wipe sampling is hazardous to the operator. Wiping articles can lead to cuts and bruises since the user must apply force to the surface. This is particularly hazardous for interior surfaces of luggage, where razor blades and hypodermic needles may be located.

6. Comparison of analytical results by the authors under operational sampling conditions showed:

a. targets that were vacuum and wipe sampled (clothing and metal lockers), the vacuum sample read higher mass present than did the wipe sample (Fortuna report to HARC Dec. 96).

b. wipe samples were positive four times when the vacuum samples were negative. In these cases the wipe sample was collected first.

c. There were no cases where the wipe sample was negative and the vacuum sample positive. This suggests that the vacuum sampler used, which used boundary layer counter contamination control, did not produce or transfer false positives. Laboratory test conducted by the authors of commercially available nozzles was a source for false positives.

7. Grouping of target samples using wipe sampling will cause cross contamination of residue from positive surfaces to clean surfaces. Vacuum sampling minimize the opportunity for transferring residue from one target surface to the another. The vacuum collector nozzle is the most likely source of this contamination.

EXAMPLES OF SAMPLING PROTOCOLS

Grouping of targets works when the prevalence of positive surfaces is low as seen in Table 1. The idea of grouping samples is to minimize the number of analysis performed by the instrument and at the same time increase sampling rates. One would group samples in sizes that would provide the probability of less than 0.5 that at least one of the group would test positive. When a group sample is negative, than no further analysis is needed. When a group sample is positive, than a new sampling strategy will be used. One such strategy if the grouping is five or less is to resample and analyze the targets individually. For larger target groups, one could form smaller groups and sample those together. Some of these groups may be negative. Groups that show positive then will require the individual targets to sampled and analyzed separately. Table 1. says that if the expected probability (prevalence) of positive targets is 0.4, that one could economically sample twenty together. If the prevalence is 0.135 (13.5% positives expected), than groupings of five can be used. If the prevalence is 7%, than a grouping of 10 is justified.

Table 1. Recommend sample group size as a function of prevalence.

GROUP SIZE	1% PREV.	4% PREV.	5% PREV.	7% PREV.	13.5% PREV.	26.1% PREV.
3	0.97	0.88	0.86	0.8	0.65	**0.4**
5	0.95	0.82	0.77	0.7	**0.49**	0.22
10	0.9	0.66	0.6	**0.48**	0.24	0.05
15	0.86	0.54	**0.46**	0.34	0.11	0.01
20	0.82	**0.44**	0.36	0.23	0.06	0

The economics of using grouping strategies for large number of items to be samples and whose expected positive rate is less than 26.1% is illustrated by the following example.

The sampling of high school lockers for illicit drugs with residue analyzers is an awesome task. Let us say, that the school contains 2000 lockers and we are to check for the presence of marijuana. The ion mobility spectrometer is an ideal analytical instrument for cocaine and methamphetamine, but it is much less sensitive for marijuana. The positive detection for marijuana requires the sampling team to analyze all samples with another technology, namely immunoassay kits designed to react to specifically to (THC) marijuana. These kits cost about $8 each. So if one were to sample each of the 2000 lockers with individual kits, the cost in kits alone would be $16,000. But, if one expected that 14% of student body were using marijuana, and of those users, half would use marijuana regularly enough to leave a residue on their lockers, then the expected prevalence is 7% (140 lockers).

Table 1. shows that a good sample size for this situation would be ten lockers at a time. Initially, 200 kits would be used at a cost of $1600. Of the 200 10-group samples 48% or 96 will test negative. Allowing the testing team to no longer have to deal with 960 lockers. However, there are 104 groups that contain at least one positive locker and the prevalence rate has nearly doubled to 13.5%. If one sampled all remaining 1040 lockers individually, the cost in kits would be an additional $8320. Thus the total cost in kits using this grouping strategy is $9,920 versus $16,000.

The savings in kits would be higher still, if a new group size were used. Table 1. suggests a logical sub group size of five. Re-sampling, in groups of five would (Table 1) means that 208 groups would be acquired and of these 100 (48.5 percent) would be expected to be zero. This step would cost an additional $1664 in kits. The remaining 108 groups of 5 lockers (5) would require individual sampling and analysis at a cost of $4,320. Thus the total investment in kits with this strategy would be $7684 versus $9,920 for the single grouping strategy. Grouping the remaining lockers by threes still would add additional savings.

The grouping strategy to sets of three requires 179 groups and $1432 in kits. Forty percent of these (71) will contain no positive lockers. This leaves 214 lockers to be sampled individually at a cost of $1928. The total cost for this strategy is $6,624.

There is another important sampling parameter that grouping of target improves is time. This is very important when screening airline baggage for explosives. The FAA has established a six second maximum time to sample a piece of luggage, have the sample analyzed, and the results interpreted. This is a very difficult time constraint. Especially, since the fastest analytical device (IMS) takes 5 seconds to analyze and interpret the sample. This leaves 1 second to sample a suitcase. Group sampling of luggage could be used to meet this condition, however.

The expected rate or prevalence of luggage containing explosive residues is most likely much less than 1 bag per 1000. We expect that the true prevalence of explosives in luggage is extremely low. But due to people who use nitroglycerin legitimately or as a heart medicine and other munitions experts, who travel we used 1 in 1000 pieces to have explosive residues at detectable levels.

This means that if we were to sample 10,000 bags, in groups of 100, with a prevalence rate of 0.001, that 99 groups will test negative and 1 group would have at least one positive piece. This also shows that the collection sampling time can be 5.95 seconds per bag, which is significantly longer than the one second per bag allowed if the bags were sampled individually.

CONCLUSIONS

1. Wipe sampling is the preferred sampling method by users of residue detectors

2. Residue detector manufacturers have pretty much ignore the sample collection and transport aspects of residue analysis

3. Vacuum sampling provides more flexibility in sample collection and transport than does wipe sampling

4. Grouping of low prevalence targets is economically justifiable

5. Group sampling is best performed through vacuum collection modules.

6. Vacuum sampling if used is best done with a boundary layer counter contamination function.

7. Collection costs are a function of the user requirement. In situations where false negatives are not critical, the protocol can be less vigorous. The high school locker sampling example shows that cost savings can be significant if group sampling is employed. Without group sampling the cost was estimated at $16,000 and only $6,624 with grouping. There many applications where these types of concepts can be employed and still meet the needs of the user.

REFERENCES

[1] Lucero, D. P. & Fortuna, J. J., "Design of a Residue-Free Hand-Held Vapor/Particle Vacuum Sampler for Trace Detection Systems,"
5th International Symposium on the Analysis and Detection of Explosives, Dec. 4-8, 95, Washington, D.C.

[2] Cliff Todd, Forensic Explosives Laboratory, Fort Halstead, Kent, England, TN14 7BP, "The Detection and Identification of Explosives Residues with Reference to Legal Proceedings," Paper #14, 5th International Symposium on the Analysis and Detection of Explosives, Dec. 4-8, 1996, Washington, D.C.

[3] Pilon, P., Dr., Hupe', M, et al, Document Scanning as an Effective method for Narcotic Interdictio, PROCEEDINGS: Counterdrug Law Enforcemtn: Applied Technolgy for Improved Operational Effectiveness International Technology Sympoium, Part 1, p 9-7, Oct 24-27, 1995

[4] Lucero, D. P. & Fortuna, J. J., "Elimination of the Residue-Contamination False-Positive Response Interferences in Trace Detection Systems Using Vacuum Samplers," 6th International Symposium On Analysis and Detection of Explosives, 6-10 July 1998, Prague, Czech Republic

The Economics of Drug Testing

By
Joseph J. Fortuna
and
Austin Lowrey, III Ph. D.

Chemical Detection Services, Inc.
7240 F Telegraph Square Drive
Lorton, VA 22079
Phone: 703 550-1806 Fax: 703 550-1808
Email: chemdet@erols.com

CHEMICAL DETECTION SERVICES, INC.

THE ECONOMICS OF DRUG TESTING

ABSTRACT

What are the economics of establishing a drug free work place? What are the criteria that one needs to consider and what are the parameters that determine cost and effectiveness of drug free workplace programs? Should a company rely solely on urine analysis as the basis of its drug screening policies? What percent of the work force should be randomly tested, if the testing rate not mandated? What are the expected economic benefits from a drug testing program? How can one determine an estimate of the prevalence of drug abuse in one's company from current test results?

These questions and others are addressed in this paper.

The authors review for the reader how much drug abuse by U. S. workers costs businesses. The paper then addresses the various testing opportunities for a company to consider. The expected payoff for various drug policies is addressed. Finally, the authors provide a decision making table for corporations to use as a guide in determining a company testing policy leading to a drug free work place.

BACKGROUND

Decisions on starting, maintaining, or altering drug free work place programs require information that most corporate managers lack. The information is not only lacking, the decision makers, in most cases, fail to realize what information is needed to make drug policy decisions pay off. As reported by the American Management Association, few companies track the benefits of drug free work place programs.

The American Management Association (Machine Office Technology, July 1996, p.23) reported that drug testing in the work place has risen 277 percent since 1987. The AMA reported [1] that eighty-nine percent of responding manufacturing firms do drug testing. Due to Federal regulations, 100 percent of transportation firms test. Seventy-nine percent of wholesalers and retailers, 73 percent of service sector businesses, 60 percent of business service providers, and 56 percent of financial service providers perform drug tests. Only 8 percent, however, have conducted cost benefit analyses.

Two percent of the respondents stated that they terminated drug testing because it was not cost beneficial. The purpose of this paper is to demonstrate that drug testing does indeed have economic value when the prevalence of drug use is two percent or higher. We start by examining the drug testing programs used today.

Respondents to the American Management Association survey [1] reported 92% use urine sampling, and 79% use no other method of drug testing. Fifteen percent use blood sampling, and 0.8% use only blood samples. Hair sampling is used by 2% of the responding companies, and 0.5% use only hair analysis. Non-medical performance testing is used by 2% of the companies, and 0.2% use only non-medical performance testing.

Urine analysis is the accepted method of drug testing in the work place. More than 90% of these tests are based on urine testing (ODD JOBS, Washington Post, P. H4, Sunday, July 28, 1996). The use of urine analysis dates from 1988 when other technologies were not available. Today, hair analysis is also available. The question is, does hair provide a benefit over urine analysis? This paper evaluates the urine and hair analyses.

According to the American Management Survey, 98 percent of all employees test negative for drugs or two percent test positive. Other surveys report that about ten percent of employees between the ages of 18 to 34, used illicit drugs [2]. In addition, SmithKline Beecham reported that 5 percent of workers tested positive for illegal substances in 1997 [3]. What does this mean? Are there really so few users that are employed, or could it be that the present testing strategies are inadequate?

A look at the reasons that 98 percent of all employees test negative for drugs begins with the validity of the estimate of the number of drug users that are employed. Two-thirds of drug users are employed (Drug Strategies, "Keeping Score," p. 20, 1995). From these statistics one could conclude that random drug screening programs would detect these users at higher percentages than are currently reported. Our analysis shows that the low detection rate is inherent in the most commonly used random sampling process, the prevalence of drug users, the type of drug abused, and the urine screening process.

ANALYTICAL METHODOLOGY

The random sampling process. Let us examine the probability that a drug user will be chosen in a random selection process. We show the effect on the selection probability as functions of work force percentage using illicit drugs (prevalence) and the random selection strategies. The prevalence of drug users and the sampling rate are the major factors in this result. There are two parameters in the random selection process. One is the percentage of people sampled per year and the second is the number of times per year that sampling is performed.

Table 1. shows the selection probability for a work force drug use prevalence of 5%, 10% and 15%. The total percentage of work forces tested yearly was calculated for 25%, 50%, 75%, 100%. For example, the fifty percent random sampling rate in our calculations means that 12.5% of the work force are randomly selected four times a year. The fifty percent sample size is required under Federal regulations. The sampling frequency is left to the employer.

Probability of a drug using employee being selected in four samples is the product of the probability of an employee being a user times the probability of being selected exactly once in four samples of 12.5% of the work force. (We assume that once employees test positive, they are removed from the sample pool. Employees who test negative may be selected more than once.)

Table 1. Probability of a drug user being selected for random urine testing.

PREVALENCE OF USERS	25% SELECT RATE	50% SELECT RATE	75% SELECT RATE	100% SELECT RATE
5% OF EMPLOYEES	0.0103	0.0167	0.0201	0.0211
10% OF EMPLOYEES	0.0206	0.0315	0.0402	0.0422
15% OF EMPLOYEES	0.0309	0.0502	0.0603	0.0603

Table 1. shows the probability of selecting a drug using employee as a function of sampling rate and prevalence of the drug use in the work force. A drug user who belongs to a low (5%) prevalence use group, can be expected to be urine tested under a fifty percent random sampling process about once in a hundred years. Is it any wonder that only 2% of those tested are found to be using drugs? Note that the probability of being selected increases with an increase in yearly sampling rates. Whether this increase is cost beneficial or not is addressed later.

The drug detection process. The next variable in the drug detection process is the likelihood that a selected drug user will have drug metabolites in his or her urine at detectable levels. Employees who use drugs at least once per day will always have detectable levels of drug metabolites in their urine. The detection of occasional users is a function of the drug used, the frequency of use, the magnitude of drug use, and the person's metabolic rate.

Except for marijuana and PCP, most drugs metabolize rather quickly. The table demonstrates why drug tests should be administered with a minimum of warning time. For pre-employment testing, advanced notice is difficult to avoid. Periodic random testing can be administered with little warning.

Table 2. Likely period after use for detection of illicit drugs in urine.

ILLICIT SUBSTANCE	DETECTION LEVEL	PERIOD OF LIKELY DETECTION
HEROIN	300 NG/ML	1-4 Days [7]
COCAINE	300 NG/ML	8-48 Hours [7]
MARIJUANA	100 NG/ML	7-34 Days [7]
LYSERGIC ACID DIETHYLAMINE (LSD)	20 NG/ML	2 Days [6]
PHENCYCLIDINE (PCP)	75 NG/ML	5-10 Days [7]

Detection probability determination process. The prevalence of occasional drug users and those who could be classified as addicts and the drug of choice brings other variables into the detection probability equation. In this analysis, we assumed that 50 percent of the drug users use drugs at such a rate that their urine is always positive. For the other 50% we used a mathematical model described in the next paragraph. For the analysis, the authors chose only marijuana and cocaine as likely drugs of abuse. Marijuana is the most used illicit drug of the two, so we assumed that 70% of the drug users would be marijuana smokers and 30% would be cocaine users. The occasional marijuana or cocaine user in this study is one who uses the drug once every seven days.

Detection Probability Model for Casual Users.

In our model, we assume that a casual user has a probability (a) of using a drug per day. We assume that this probability (a) is constant and independent of time. These assumptions define the applicability of the Possion statistical probability distribution:

$$P_n(t)=[(at)^n/n!]e^{-at}$$

Where $P_n(t)$ is the probability that a person has used the drug exactly n times from time zero to time t, where n! is the mathematical expression for n factorial, and e is the base for natural logarithms. In particular, $P_0(t)$ is the probability that a person has not used the drug from time zero to time t. And 1- $P_0(t)$ is the probability that a person has used a drug at least once in the last t days.

For occasional marijuana users: Using an average time between usage as seven days, probability of use per day is 0.14. Using the seven day detection window from Table 2., the probability that a person used marijuana and whose urine exceeds urine test thresholds in the last seven days is 0.62.

For occasional cocaine users: Using an average time between occasional cocaine use as seven days , probability of use per day is 0.14. Using the two day detection window from Table 2., the probability that a person used cocaine and whose urine is at a level exceeding urine thresholds within the last two days is 0.44.

RESULTS OF ANALYSIS

The results are summarized in Tables 3, 4, and 5. Table 3. shows the probability of a marijuana user being selected and failing a urine test as a function of prevalence and sampling strategies. Table 4. shows the probability of a cocaine user being detected as a function of prevalence and selection strategies. Table 5. is the probability that either one would be detected, again as a function of prevalence and sampling rate.

Table 3. Probability of a marijuana user being selected and failing a urine test.

PREVALENCE OF MARIJUANA USERS	25% SELECT RATE	50% SELECT RATE	75% SELECT RATE	100% SELECT RATE
3.5%	0.0058	0.0095	0.0114	0.0120
7 %	0.0117	0.0190	0.0228	0.0239
10.5%	0.0175	0.0285	0.0342	0.0359

Table 4. Probability of a cocaine user being selected and failing a urine test.

PREVALENCE OF COCAINE USERS	25% SELECT RATE	50% SELECT RATE	75% SELECT RATE	100% SELECT RATE
1.5%	0.0018	0.0029	0.0035	0.0046
3%	0.0036	0.0058	0.0087	0.0091
4.5%	0.0067	0.0108	0.0130	0.0137

Table 5. Probability that either a marijuana or cocaine user will be detected.

PREVALENCE OF ALL USERS (MJ OR COCAINE)	25% SELECT RATE	50% SELECT RATE	75% SELECT RATE	100% SELECT RATE
5%	0.0076	0.0124	0.0149	0.0165
10%	0.0036	0.0248	0.0315	0.0330
15%	0.0242	0.0393	0.0427	0.0495

Table 5. is the sum of Tables 3. and 4. The tables were generated independently and the values may differ from the expected sums due to rounding. Table 5. shows that if ten percent of a work force uses marijuana or cocaine, then the company that randomly tests 50% of this work force, and samples these four time a year, will expect to catch about three people for every one hundred sampled, or a three percent positive rate. If it costs a company $100 to test each employee, then the cost to test 100 people is $10,000. This raises the question is it worth $10,000 to a company to catch three drug abusing employees? Is there economic benefit in random urine testing? This is the question raised by the American Management Association.

A drug user costs a company about $7500 per year [4]. These costs are due to loss in productivity, accidents, tardiness, absenteeism, theft, worker compensation claims, etc. Thus a prevalence of ten percent of drug users in a work force will cost a company $75,000 per year per hundred employees. The expected value of the random drug testing program is the product of the expected number of people caught times the total cost of having drug abusing employees. In this illustration the expected number of people caught is 2.48 per 100 tested with an expected savings of $18,600 for an investment of $10,000 per one hundred employees. The pay off is $1.86 for every dollar invested. The cost for having a drug abusing employee must be below $4,032 per year before drug testing is financially a poor policy with this strategy.

How do other random testing strategies affect this payoff? How does sampling higher or lower percentages affect this pay off? How does the frequency of performing the tests affect this payoff? These questions are addressed below.

CHEMICAL DETECTION SERVICES, INC.

SAMPLING RATE EFFECTS ON EXPECTED PAYOFF

Table 6. shows the expected pay off for sampling at four different rates, four times a year:

6.5 employees per hundred (25%),
12.5 employees per hundred (50%),
18.7 employees per hundred (75%), and,
25.0 employees per hundred (100%).

Prevalence rates of five, ten, and fifteen percent were used. An estimated cost of $100 per sample was used based on laboratory cost, program costs, and lost of productivity costs. Table 6. shows the expected payoffs for four sampling rates and the three prevalence rates. The payoff is the difference between the expected savings per test and the estimated cost per test.

Table 6:
The expected payoff of drug testing as function of percent sampled four times per year.

PREVALENCE OF USERS	25% SELECT RATE	50% SELECT RATE	75% SELECT RATE	100% SELECT RATE
5% USE MJ OR COCAINE	-$42.78	-$6.95	$11.75	$23.87
10% USE MJ OR COCAINE	$14.44	$86.09	$136.24	$147.75
15% USE MJ OR COCAINE	$81.45	$195.06	$254.36	$271.62

Two conclusions were made from this payoff chart. One, with low prevalence rates, random sampling of 50% or less is financially a bad policy. Two, sampling a large percentage of the work force pays higher returns. For example, sampling seventy-five percent of a 5% prevalent work force would return about $12, while the 25% and 50% sampling rates have negative returns. The conclusion then is to sample at high percentage rates. In fact, a sampling strategy of 100% has the best pay off down to prevalence rates less than two percent. Below two percent no strategy has an expected positive payoff.

A company with an estimated drug prevalence rate of less than 2% would test for reasons other than a cost savings. Regardless, 100% testing would result in the highest payoff policy.

SAMPLING FREQUENCY EFFECTS ON EXPECTED PAYOFF

How often should one conduct random sampling? One, two, three, four or more times per year? Based on this statistical analysis, the authors conclude that it is best to test once per year and to test everybody. This strategy ignores the deterrence affects of multiple sampling. The perception is that if multiple samples of the work force is taken periodically, than a user is more likely to be selected and detected as a user. Actually the chance of being selected and detected is much higher if 100% testing is performed. This is due to the affect of sampling the work force with replacement. This is a mathematical way of saying that an employee is put back into the selection pool and may be tested more than once per year and some employees may not be selected at all, even with 100% (25% four times a year) selection rates. The chance that an individual is selected at least once under these conditions is 0.68 which means that a user has a 32% chance of not being picked to be tested!

The most efficient random program is based on the randomness of choosing the one day to sample everybody and not on how many and when to sample smaller groups. Figure 1. shows the effects of sampling frequency. The Y-axis is the probability of detecting users and the X-axis is the number of times per year the sampling is conducted. Figure 1. is based on a prevalence of five percent and a sampling strategy of 50% of work force per year with replacement.

This recommendation does not take into account the affect of that multiple sampling has as a deferent to the work force. One could assume that if the employees know that they will be tested only once a year, then they will tend to abuse drugs more after the yearly test is conducted. The counter to that is that it is most likely that addicts or users that require at least one dose per day will continue to use drugs regardless of the corporate policy. The hard core addict or user is the user who most likely will cost a company money.

The recreational user will continue to use drugs occasionally and will be very difficult to detect. These occasional users, if impaired at work, are best detected by the observations of their supervisors and reports by fellow employees. Once a year testing will catch the addicts or the more than one dose a day user and some of the occasional users. The recommended sampling selection policy incorporates stratification of the employee population by risk of being a user. This is explained in the next section.

EMPLOYEE SAMPLING STRATIFICATION

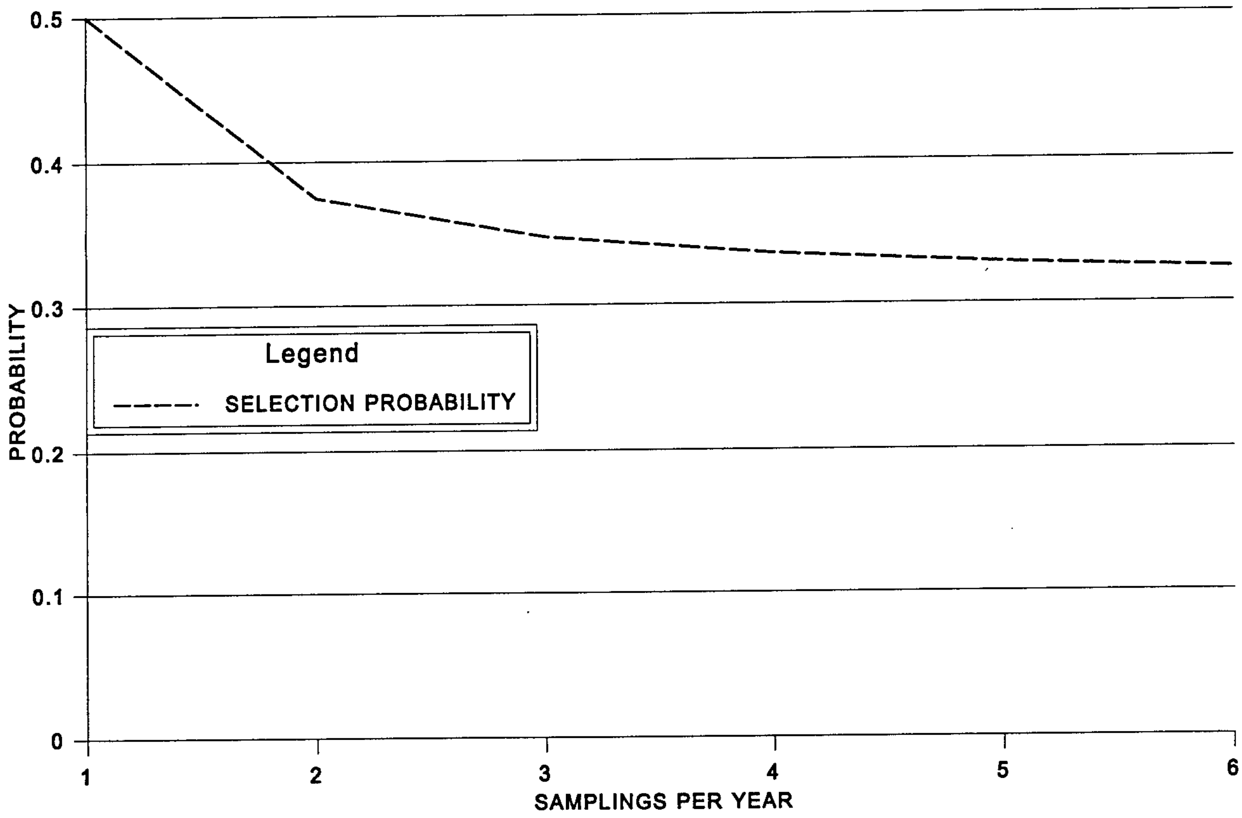
Stratification process. Establishing employee sampling strata and sampling each population based on degree of risk was analyzed by the authors. We found that stratification is easily achievable and cost effective. Three employee sampling categories were developed based on urine and hair testing analyses results.

The established Federal (SAMHSA) urine cutoff levels (thresholds) were developed by manufacturers to produce optimum performance of urine test kits [8] thresholds independent of impairment levels. Hence, for drug testing a non-mandated company can ignore thresholds and should request its drug testing laboratory to test urine down to the lowest detection level of their

GC/MS (gas chromatograph/mass spectrometer).

SAMPLING FREQUENCY EFFECTS

FIGURE 1



The results from these tests can allow one to arrange employees into different groups whose sampling rate differs by the degree of risk an employee represents to the company. For example, if an employee is tested two times and no illicit drug metabolite is presence in the specimen, than this employee could be sampled less frequently, say 25% rather than 50% random pool as required by the Department of Transportation [9]. An employee who had at least one urine sample show presence of illicit drug metabolite, but below the Federal guidelines, could be put into a pool of tested at 100% until a string of negatives test results are achieved. Employees whose urine contains metabolites exceeding the Federal cutoff levels will need to be put into a third group and tested more frequently and 100%.

The use of hair as a specimen adds even more criteria [10] for drug testing stratifications in a work force. Hair provides an observation period of about 60 to 90 days [5]. The use of hair analysis results greatly increases the likelihood that a person whose hair and urine contain no drug metabolites is not an user.

This employee is placed in a low prevalence group with a low percentage of sampling. The low sampling policy is more of a deterrent to thwart future use, rather than one based on cost benefit. The payoff value of using both urine and hair is shown in Table 7.

Table 7. Payoffs using hair and urine testing.

PREVALENCE OF USERS	25% SELECT RATE	50% SELECT RATE	75% SELECT RATE	100% SELECT RATE
5% USE MJ OR COCAINE	-$23.52	$24.35	$49.35	$56.62
10% USE MJ OR COCAINE	$52.95	$148.71	$198.69	$213.24
15% USE MJ OR COCAINE	$129.42	$273.06	$348.04	$369.86

Comparing Table 6. (Payoff with urine only) and Table 7. (payoff with urine and hair) shows the expected added return of using both specimens. The payoff for using both hair and urine is approximately double that of a program based solely on urine analysis.

The authors have developed an employee stratification program which is a far more effective selection, detection, and ultimately deterrent than the present day concept of random testing based solely on urine specimens. We place employees into one of three risk categories. (Risk meaning the likelihood that they are drug users.)

The three categories of employees are:

Very low risk employees (prevalence rate close to zero),
Moderate risk employees (prevalence rates close to 100%), and
High risk employees (prevalence rate at 100%).

CHEMICAL DETECTION SERVICES, INC.

The groups are defined by:

Test all employees at least twice in one year
Collect and analyze urine and hair specimens
Analyze all specimens at established threshold standards
Analyze all negative specimens to lower detection limit of GC/MS
Category 1 employees: Employees whose urine and hair analyses contain no illicit drug metabolite after two tests.
Category 2 employees: Employees whose urine or hair contains illicit drug metabolite at levels below thresholds.
Category 3 employees: Employees whose urine or hair contains illicit drugs above the threshold levels.

Employees in the low risk group will be selected for drug (urine and hair) testing at a 25% rate, four times per year (6.25% each selection). This is for deterrence only. The cost for this program will exceed the expected value.

The employees in the moderate risk group will be tested (urine and hair) four times a year, with 100% sampling each selection. The employees in the high risk group will be tested weekly.

Testing the total work force of a hundred employees twice in six months would cost $20,000. The expected payoff for identifying the ten illicit drug users from this strategy would be $75,000. Assuming that the prevalence rate is 10%, then the expected number of employees who would screen negative with urine and hair wold be 90. These employees will tested at a 25% rate the following year at a cost of $2250. Assume that of the ten employees tested, those who were above the lower detection limit and below the urine or hair thresholds number five. These five people would be tested four times a year, 100% each sample at a cost of $2000. The remaining five people, who tested above the urine or hair thresholds), would be tested weekly with urine specimens. Again the lower detection limit of the GC/Ms would be used, i.e. no cut off thresholds. This would continue until either the employee's urine were completely clean or until the employee was removed from the work force.

For water soluble drugs such as cocaine, we estimate that zero levels of metabolite should be expected after two weeks. The metabolite for marijuana would take about six weeks to disappear from the urine. The levels of metabolites should be decreasing or at most staying level on weekly test results. The expected cost of this program is $3000. Once an employee tests negative down to the lower detection limit of the GC/MS. these five employees would be retained in the high risk category and be subject to testing four times a year at a cost of $2000. Employees, in the moderate risk level strata can be placed in the low risk population only after two years of negative metabolite readings in either urine or hair. Employees who are placed into the high risk group from the moderate risk group will be tested weekly for six weeks.

The first year cost of the program is $27,250 with an expected payoff of $47,750. Assuming, the prevalence rate drops to five percent with this program, the second year cost are $2375 for the low risk group, about $1200 for the moderate risk group, and $1800 for the high risk group. This totals $5375. Thus the expected pay off would be ($37,500-5,375) $32,125.

This compares favorably to the cost benefit of 50 percent random testing without stratification. Using Table 6., which says the expected payoff would be $8,609 per year or $17,218. The employee sample stratification is practical and cost effective.

Reasonable suspicion and post accident testing is still recommended for all employ sampling groups. Reasonable suspicion testing is testing that is conducted on a specific employee because a trained observer (supervisor) has detected behavior, odors, or impairment. The supervisor needs to be trained in detect signs of both drugs and alcohol abuse. This training, and the policy of reasonable suspicion testing, is recommended.

ESTIMATING PREVALENCE FROM HISTORICAL TEST RESULTS

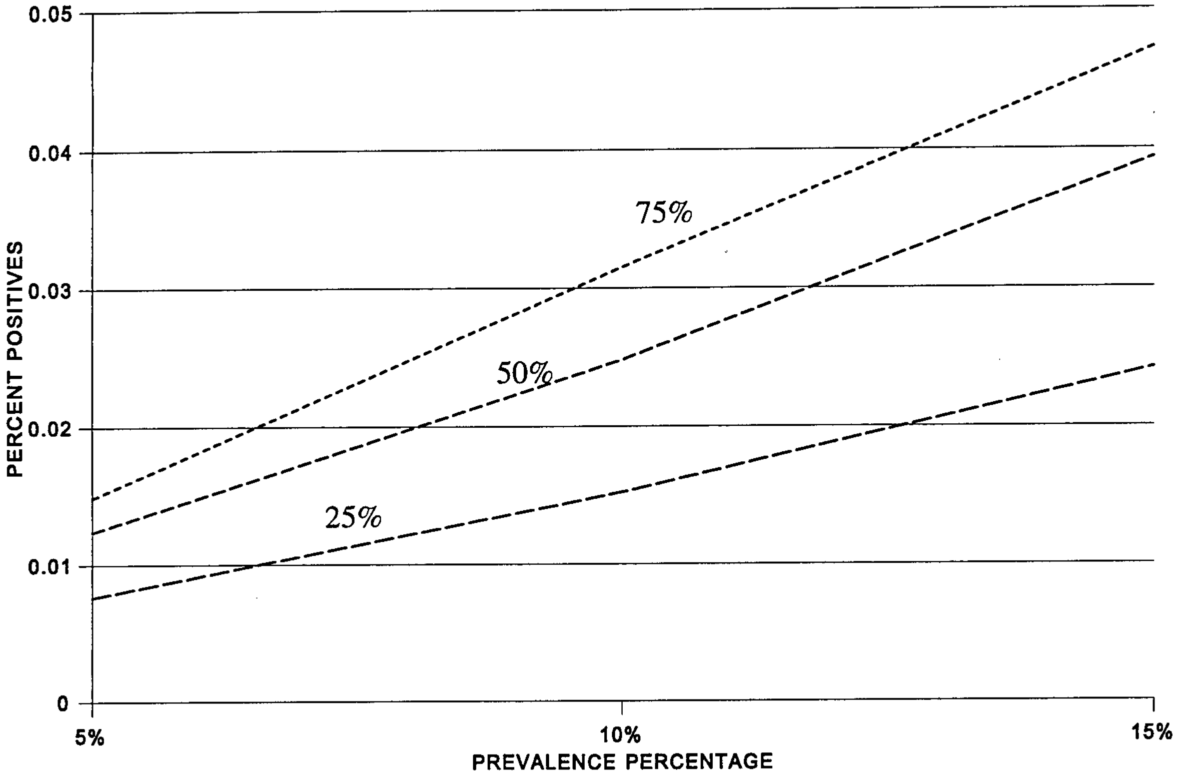
How is a company to know its prevalence rate for drug abuse? Once you test, or if you tested in the recent past at either a 25%, 50%, or 75% rate, Figure 2. can be used to provide you with an estimate of prevalence in a company. Returning to the American Management Association study that reported a 2% positive rate, one could use Figure 2. and estimate that population of users in this survey.

The Y-axis of the chart is the detection rate experienced. For a 75% selection rate the prevalence of users is estimated at 6.25%. For 50% and 25% selection rates the prevalence is estimated at eight and 12.5% respectively. This chart was based on a number of assumptions and these limit any precision in the estimate. However, the model will provide a decision maker with an estimate that could be used in establishing drug policy changes.

CHEMICAL DETECTION SERVICES, INC.

PREVALENCE PREDICTOR

FIGURE 2



CONCLUSIONS

Drug testing programs used today can be greatly improved. Both urine and hair should be used with detection of metabolites reported above the lower detection limits of the GC/MS for all sample specimens. Stratification of employees into statistical risk groups is easily accomplishable and has extremely large payoffs. Prevalence in a work force can be estimated by using historical testing results data and a simple graph developed by the authors.

CHEMICAL DETECTION SERVICES, INC.

RECOMMENDATIONS

Refinements to the prevalence predictor model should be made by including more than the two drugs chosen by the authors. Data on heroin, methamphetamine, and PCP abuse should be included to ensure a more accurate prevalence estimate. More accurate and extensive data on metabolite concentrations as a function of time after use is needed to improve the detection probabilities estimates. Cost benefits of using employee sampling stratification needs to perform on a test population of employees along with a control group.

CHEMICAL DETECTION SERVICES, INC.

BIBLIOGRAPHY

[1] 1996 AMA Survey Workplace Drug Testing and Drug Abuse Policies, Summary of Key Findings, Research Report, American Management Association, 135 West 50th Street, NY, NY 10020-1201

[2] Investing in the Workplace, Drug Strategies, 2445 M Street N.W., Suite 480 Washington, D.C 20037, p. 2

[3] "Annual Survey Shows Workplace Drug Use Down From 1996", Workplace Substance Abuse Advisor, Vol. 12, No. 10, p. 1, Apr., 23 '98.

[4] "Keeping Score," Drug Strategies, 2445 M Street N.W., Suite 480 Washington, D.C 20037., 1996, p. 17

[5] Kidwell, D. A., Ph.D., "The Alternative Matrix Program for Drug Abuse Detection and Deterrence", ONDCP/CTAC Drug Abuse Treatment Technology Workshop August 1995, Proceedings, p.3.13-3.36

[6] Papac, D. I. & Foltz R. L., "Measurement of lysergic acid diethylamine (LSD) in human plasmas by gas chromatography/negative ion chemical ionization mass spectrometer", Journal of Analytical Toxicology, V14n3, May-June 1990, p. 189-190.

[7] Uthman, E. O. Diplomate, American Board of Pathology, April 1993

[8] Berkable, D. R., Institute News, American Toxicology Institute, Inc., Mar/Apr 98, 3330 Sunrise Ave., Suite 110, Las Vegas, NV 89101

[9] Code of Federal Regulations, 1994, 40.29

[10] Fortuna, J. J., Fortuna, P. B., "Keys to a Drug Free Work Place", SPIE Conference 2932A, Boston, MA.,19 Nov. 96, Vol 2932.

Installation and Auditing of Security Technology

Session IV: Technical and Policy Focus Groups
Group B

Peter J Crook*, Robert M Rodger,
Flight Sergeant Barry Connell RAF

Police Scientific Development Branch
Home Office
Langhurst House
Langhurstwood Road
Horsham
West Sussex
RH12 4WX
United Kingdom

Tel: +44 1403 255451
Fax: +44 1403 213827
Email: pcrook@langhurst.org.uk

Abstract

Successful organisations and companies aim at value for money in all aspects of their business, including security.

Concentrating mainly on equipment to improve an organisation's physical security will not necessarily ensure that the resulting system will be effective. Realistic performance criteria should be used in specifying countermeasures against existing and potential new threats. Serious thought should also be given to the training of the operators and the writing of clear and effective operating procedures.

Security system auditing against the identified requirements should be undertaken shortly after the system is installed then carried out regularly to ensure that the system continues to meet the performance requirements and therefore that the initial investment on the system is proving worthwhile.

This paper offers guidance on achieving value for money in procuring and installing a physical security system. It also describes the skills required to audit perimeter security systems. It uses lessons learnt from a diverse range of projects, including some from work directed towards protecting critical national infrastructures in the United Kingdom

Introduction

The Police Scientific Development Branch (PSDB) of the Home Office has for many years been advising, assisting and developing security strategies and technologies for industry and government use. This has meant working closely with the oil and gas industry, the power generation and distribution utilities, the water supply companies and with government departments. Work has been carried out with the Prison Service to enhance the security regimes within prisons.

In July 1996 President Clinton called into being the President's Commission on Critical Infrastructure Protection[1] (PCCIP) which reported in October 1997. This was to develop a strategic approach to the protection, both current and postulated, of the United States critical infrastructures. The PCCIP combined security expertise from both government and industry in the exercise. In the United Kingdom a similar exercise had been carried out many years previously, co-ordinated through the Cabinet Office, that has looked at Economic Key Points (EKP).

Several of the findings of the PCCIP correspond closely with our views. It may be argued that Britain is several years ahead of the US in the implementation of counter-terrorist measures and this paper is designed to share, from this perspective, some of our experiences.

Threat, Asset and Vulnerability

If an organisation decides to spend money on security, it should carry out some form of risk assessment to ensure that the money is spent wisely. So, as a first step, the organisation should determine its assets, the threats against them and the vulnerability of these assests to disruption. The organisation's managers should be realistic when addressing these issues, irrespective of the organisation's size or business area.

For each of the three areas; threat, asset and vulnerability, specific information should be sought and analysed:

1. Threat.
   What are the threats, their likelihood and frequency?

2. Asset.
   For each asset, what are the implications of loss both in terms of criticality and cost but also how easy is the assest to replace or bypass?

3. Vulnerability.
   What are the immediate and peripheral vulnerabilities of the assets?

Only when all three of these aspects are assessed can it be judged whether there is a security problem that needs addressing. A useful by-product of this Risk Assessment process is that a disaster recovery or contingency plan can be produced with little additional effort.

"A terrorist bomb is only one of a number of possibly disastrous threats which a business faces nowadays. In many respects a serious fire, flood, or a catastrophic failure of a company's IT infrastructure, may be as damaging to the business as the consequences of a bomb explosion. A Business Continuity Plan should be drafted in such a way as to cover all risks."[2]

"Managers are increasingly coming to recognise that disaster recovery planning is an essential function in the management of the business. This is not surprising. Studies have shown that about 80% of companies which do not have a workable recovery plan will fail within one year of suffering a major disaster."[2]

The British Government has been developing a methodology, known as "Baseline Measures" to improve value for money, reduce costs and make security more objective.

The baseline measures approach considers assets as tangible (information, equipment, people, buildings and commodities) and intangible (morale, reputation etc.). This methodology also considers threats as traditional (espionage, terrorism, theft, insider etc.) and non traditional (fire and flood). Thus a thorough and penetrating examination of a business's security needs can aid the long term survivability of that organisation.

Operational Requirement and Performance Specification

The procurement process should aim to deliver a system which matches the needs of the organisation. This should be carried out only after the risk assessment has been completed, and security enhancements are deemed necessary. The next step, after the high level risk assessment, is the development of specific operational requirements for specific assets or vulnerabilities.

An operational requirement (OR) can be defined as a statement of needs based on a thorough and systematic assessment of the problems to be solved and the required solutions[3]. But what does that mean? In PSDB, the OR methodology was initially designed to take prospective customers through the minefield of procuring closed circuit television (CCTV) systems for deployment in an urban environment. However, the concept can be applied to any form of procurement from paperclips to battle-tanks. It relies on a partnership between the customer and an OR facilitator to address the actual security problems, which may differ from the perceived problems.

The customer (this term may cover more than one project stakeholder) is taken through a series of questions relevant to the problem. We have developed question sheets for CCTV deployment in urban areas, military establishments and penal institutions. These prompt the customer to focus on specific issues and to decide whether or not they are relevant. It is essential that the OR is "customer driven" and that the facilitator acts as the "interpreter" of technical information that the customer may not fully understand. The facilitator must not offer "his" solution to the customer but remain detached from offering any opinions, no matter how well founded.

Once the OR has been written and all parties who have contributed to the production of the document have agreed on its format and content, the OR is given to the "technical expert". It is his or her job to translate the OR into a performance specification (PS). A PS is used to determine whether the performance of a system is sufficient to meet the needs of the OR. The PS should be based on objective and measurable figures of merit which relate to mandatory functions required by the OR. Included in the PS should be a set of measurable standards which fulfil two basic functions:

1. to help the potential contractor understand exactly what the customer requires; and
2. to provide a rejection mechanism if the end product does not conform adequately to the PS, i.e. to enable the customer to withhold payment, if that becomes necessary.

The PS should then be included in an Invitation to Tender (ITT) and sent out to selected contractors for them to offer their design solution to the problem and the relevant costings. Selection of the contractor to carry out the work should ideally be taken on merit, and not just cost.

Acceptance Tests

It should be ensured that throughout the system installation process, the Project Manager monitors progress by liaising with the Contractor. Before "accepting" the finished product, the customer must ensure that it has been installed correctly and performs in accordance with the performance specification based upon the operational requirement. This phase of the project is the acceptance or commissioning testing and is where the value of using measurable standards becomes evident.

The contractor should be clear that once he has stated that the system is ready for testing, any subsequent failure to meet the agreed standard may lead to the system being rejected. Included in the PS will be the standards to be tested, the levels to be achieved, the method of testing and the test equipment to be used. Choice of test equipment can sometimes be a contentious point with the contractor and customer each preferring to use their own instruments. It is essential that whichever instruments are used, that they should properly calibrated and certified as such. Multimeters should sample at the same rate and have the same features; lightmeters should be colour corrected (if applicable); a standard test target should be used for determining target height or picture resolution in a CCTV system, etc. Any failure to have or specify a test procedure gives the contractor the potential not to satisfy the PS, at no penalty.

> At one establishment a contractor had been requested to provide twelve cameras on poles in order to view the perimeter. The establishment was provided with exactly what they had asked for, twelve cameras on poles. However, the cameras were installed without power or any image transmission system. There was presumably an intimation of what was really required but because of the lack of a PS, the establishment did not have any means for rejection of this inadequate system. Further expense was incurred in order to remedy the situation.
>
> In contrast, PSDB placed a contract to install twenty eight cameras within a prison establishment. The installation had to be carried out to a high specification because the cameras were to be used with a sophisticated video motion detection system. When the installation failed the acceptance tests, the contractor was given the test information and the reasons for failure. After several attempts by the contractor to remedy the situation the contract was terminated. Excuses querying whether PSDB could expect a contractor to meet some of the requirements did not carry weight. The contractor had read and accepted the PS and had contractually agreed to meet the requirement. Another contractor was engaged to finish the installation.

Without testing against the measurables listed within a PS, the customer may be left with no option other than to accept a sub-standard system.

Equipment, People and Procedures

It is vital to understand that any security system is only as good as the elements that make it up. In addition to the equipment, such as detection systems, closed circuit television and lighting, there is a need for competent operators and well written procedures.

There is little point in deploying "state of the art" hardware, procured using a performance specification, without having carefully drawn up operational procedures. Nor can management expect an effective system where there is good hardware and procedures controlled by poorly trained or badly motivated operators.

System managers often lose sight of the importance of operator training. However, an operator's performance will be a key determining factor in the overall effectiveness of the system. PSDB has developed guidance[4] for the selection and training of operators of closed circuit television systems. The value of this guidance has been demonstrated in pilot trials.

Maintenance Testing and Auditing

Effective programmed maintenance can be carried out only if a maintenance contract or schedule has been set up.

> Q: Why do we need to maintain our system?
> A: To ensure that when required the system performs to meet the need.

The level of maintenance required should be identified in the OR and included in the PS. An effective maintenance schedule should comprise weekly, monthly, bi-annual and annual tasks carried out by a combination of technical and non technical personnel.

Just like the acceptance tests, specific aspects of performance should be measured against previously set standards. An audit is a series of checks, designed to test whether a system's performance meets the OR. The results of one audit should be comparable with previous test results, allowing managers to identify even a small deterioration in equipment performance. Any significant changes in results indicate that there is a problem to be addressed. Correcting these deficiencies when they are discovered protects system owners from the embarrassment of discovering a weakness during or after a "real" incident.

> An establishment which used CCTV cameras, placed within the sterile zone, around its perimeter had a camera which had failed. The camera was replaced by the contractor and the camera pole was re-erected. The view along a sterile zone looked very much the same regardless of which camera it was being viewed from. It was only during a maintenance test that it transpired the camera had been replaced

pointing the opposite way from the original. This created a whole zone where an attacker could have crossed without being seen.

Assuming that the customer's needs for the system have not changed then an audit team need be familiar only with the system PS. Audit teams should work rigorously and systematically through each of the tests required to be carried out. It is important that members of the audit team have no vested interest in the outcome of the audit. It is advisable for the team to be engaged from an outside organisation for tests. No special skills are required to conduct an audit but it is necessary that the team is fully able to conduct each separate test required and understands fully the implications of test failure. Familiarity with the system's function, before any tests are started, should speed up the auditing process and help to eliminate any errors. The audit team should report their work in writing, clearly and concisely and, if necessary, diplomatically.

Testing Systems

All parts of the security system, the equipment (barriers, detection systems, closed circuit television, security lighting and access control technology), the people (operators and response forces) and the procedures all need to be tested to confirm compliance with the customer needs. Only when the needs have been addressed and the security solutions have been appropriately implemented can we expect that "value for money" is to be obtained.

References

1) President's Commission on Critical Infrastructure Protection
1997

2) Business as Usual
Home Office
www.homeoffice.gov.uk

3) CCTV Operational Requirements Manual
J Aldridge
PSDB Publication 17/94

4) CCTV: Making it Work
Training Practices for CCTV Operators
C Diffley, E Wallace
PSDB Publication 9/98

STS

SENSOR
TECHNOLOGIES &
SYSTEMS, INC.

7655 EAST REDFIELD ROAD, SUITE 10
SCOTTSDALE, ARIZONA 85260, USA
(602) 483-1997
(602) 483-2011 FAX
www.sensor-tech.com

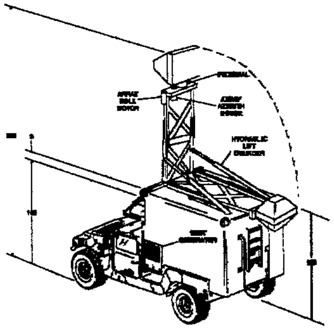
STS SENSOR TECHNOLOGIES & SYSTEMS, INC.

SENSOR TECHNOLOGIES & SYSTEMS, INC.

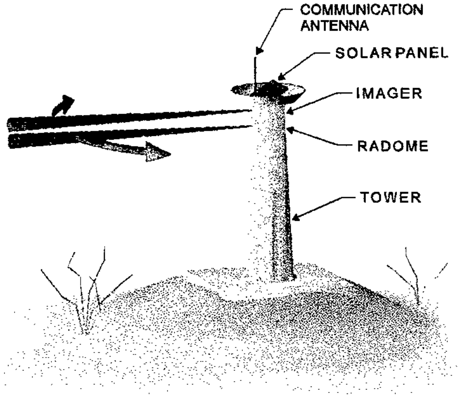
- HEADQUARTERS:
  - ◆ 7655 EAST REDFIELD ROAD, SCOTTSDALE, ARIZONA 85260
- CAPABILITIES:
  - ◆ SPECIFICATION, DESIGN, FABRICATION & TEST
    - RADAR AND RF SYSTEMS AND SUBSYSTEMS
    - ACTIVE AND PASSIVE MISSILE SEEKERS
    - SURVEILLANCE AND TARGETING SYSTEMS
    - SIGNAL PROCESSORS
  - ◆ MODELING AND SIMULATION
    - RADAR SYSTEMS
    - INTELLIGENT TRANSPORTATION SYSTEMS
    - MISSILE GUIDANCE SYSTEMS
    - GIMBALS / ANTENNAS
    - 6-DOF (GLINT/CLUTTER/MULTIPATH)
  - ◆ FIELD AND CAPTIVE FLIGHT TESTING
- CERTIFICATIONS:
  - ◆ DCAA AUDITED RATES
  - ◆ DCAA ACCOUNTING SYSTEM
  - ◆ SECRET FACILITY AND PERSONNEL CLEARANCES

SENSOR TECHNOLOGIES & SYSTEMS, INC.

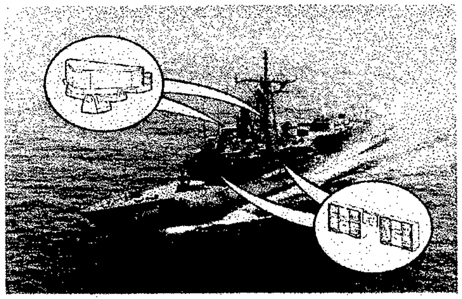
STS FAMILY OF SOLID STATE RADARS



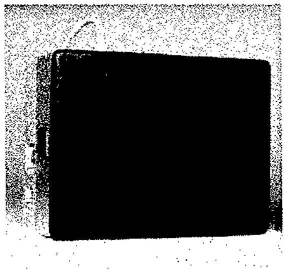
LowPAR



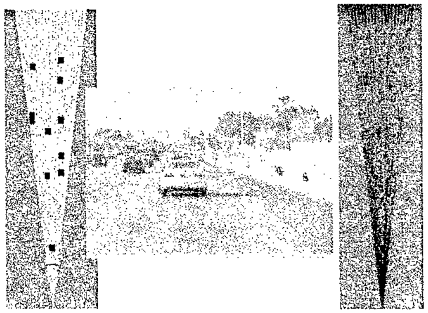
SENTRY



CAMBR



PRESENCE/MOTION DETECTOR



LOW COST IMAGER

KINGFISHER

STS SENSOR TECHNOLOGIES & SYSTEMS, INC. COMARCO

THE SENTRY SYSTEM

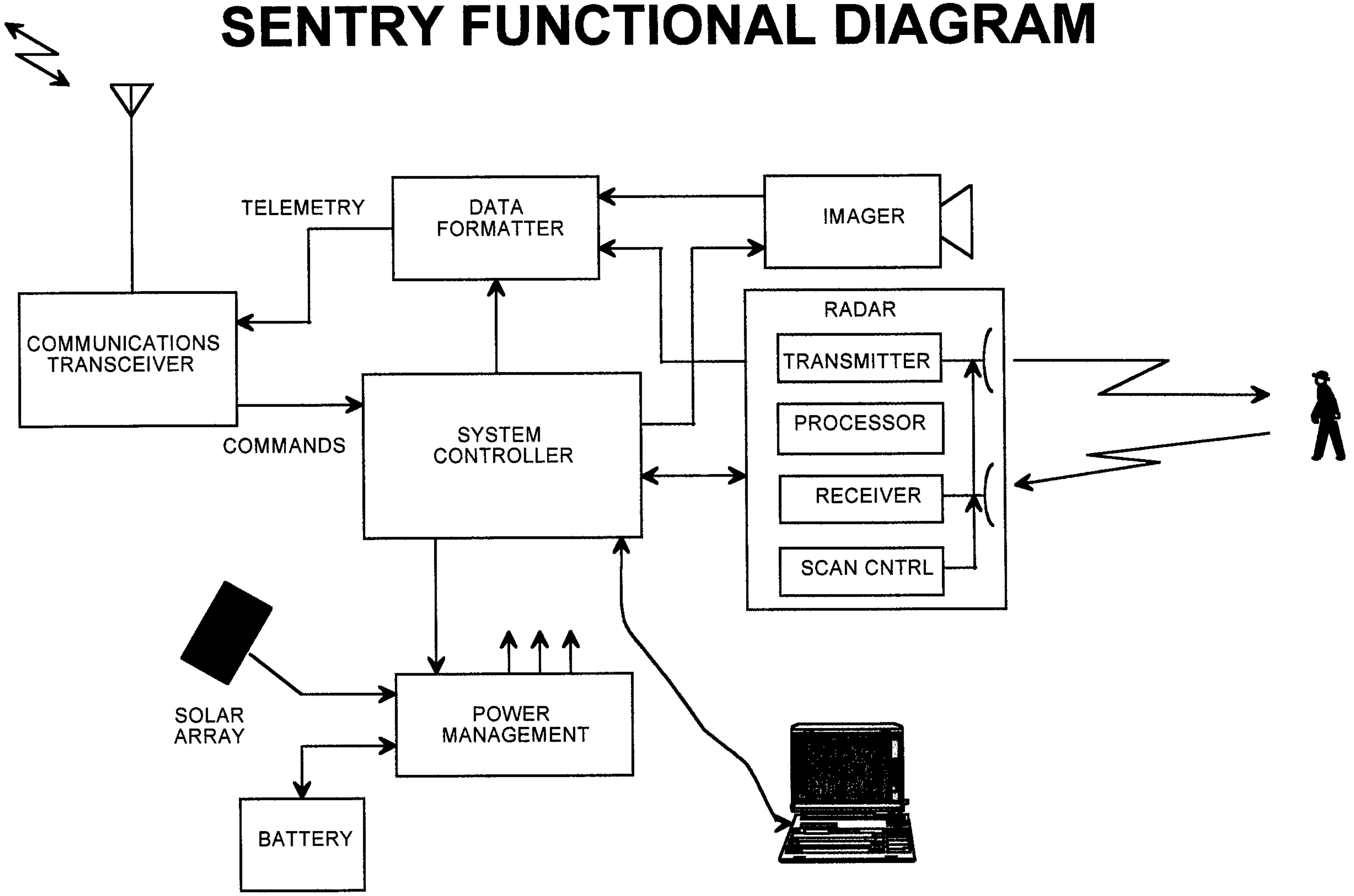
- PROVIDES BOTH WIDE AREA AND HIGH RESOLUTION SURVEILLANCE FOR BORDER SECURITY AND FORCE PROTECTION
- COMBINATION OF LOW COST RADAR AND IMAGING SENSORS
  - ◆ RADAR PROVIDES INITIAL MOTION DETECTION
  - ◆ IMAGER ELIMINATES FALSE ALARMS FROM ANIMALS
- SENSED ACTIVITY DATA (RADAR AND VIDEO) TRANSMITTED TO COMMAND POST FOR VERIFICATION AND RESPONSE DECISION
- BOTH FIXED AND MOBILE SITES
  - ◆ FIXED SITES HARDENED AND SOLAR POWERED
  - ◆ MOBILE SITES CAN SERVE AS MINI COMMAND POSTS
- OVERLAPPING NETWORK PROVIDES CONTINUOUS COVERAGE
- SAME BASIC UNIT FOR SITE SECURITY, BORDER, PERIMETER AND COASTLINE SURVEILLANCE

ADVANTAGES OF ADDING RADAR TO IMAGING SYSTEMS

- AUTOMATIC MOTION DETECTION
- SIMPLE WIDE AREA SURVEILLANCE - TARGET RANGE
- MULTIPLY MANPOWER EFFECTIVENESS
- ALL WEATHER, ALL LIGHT LEVEL DETECTION
- NO NEED TO TRANSMIT DATA UNTIL MOTION DETECTED
- INCREASED COVERAGE CAN REDUCE NUMBER OF SITES

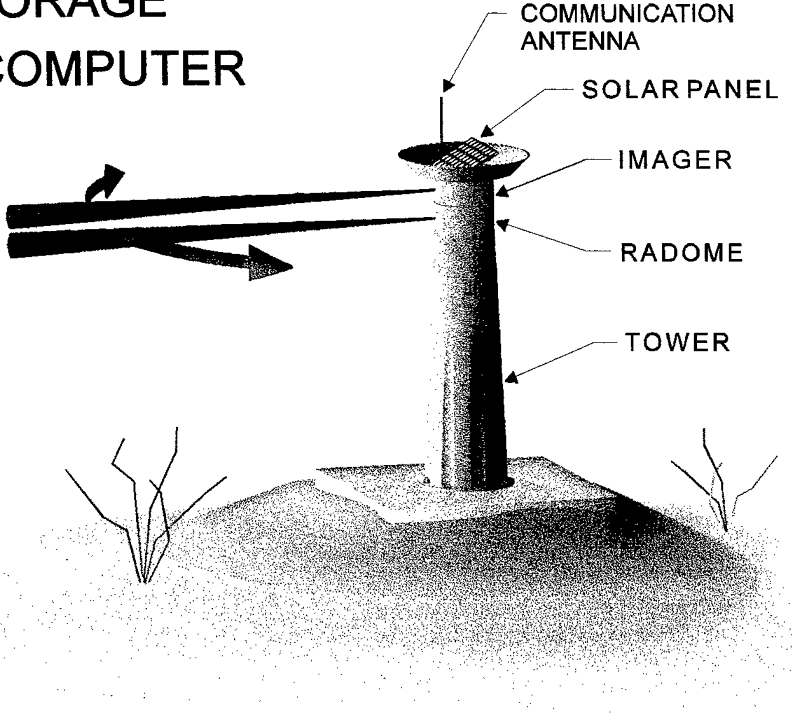
STS SENSOR TECHNOLOGIES & SYSTEMS, INC. COMARCO

SENTRY FUNCTIONAL DIAGRAM

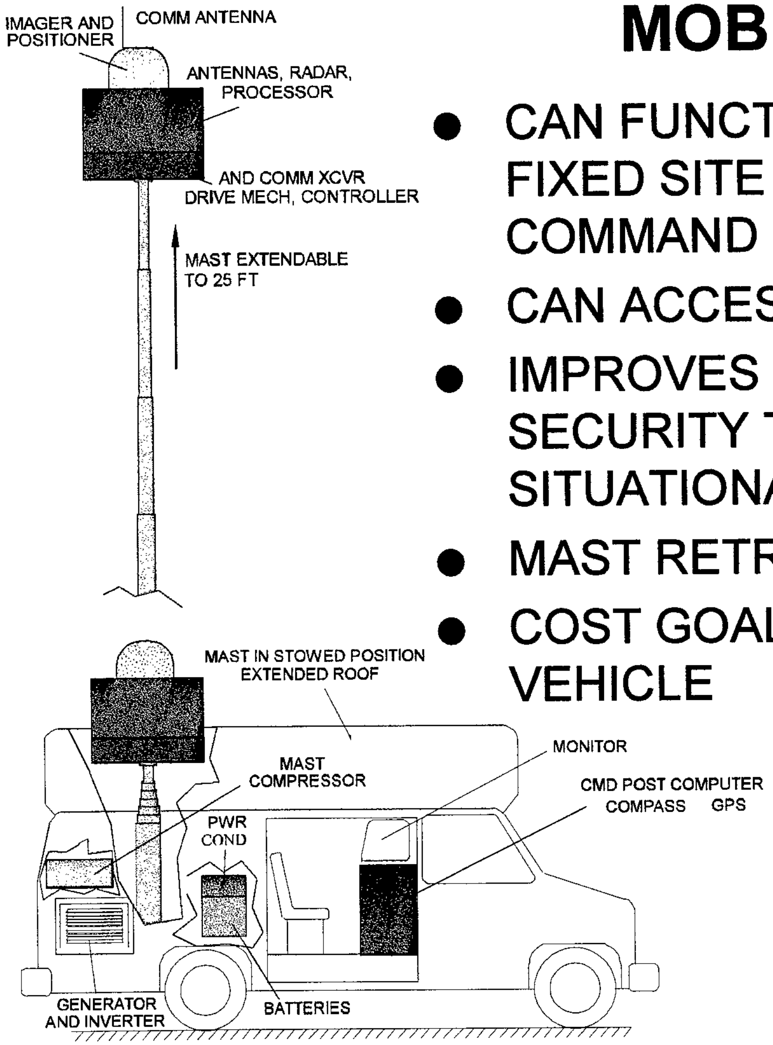


FIXED SITE

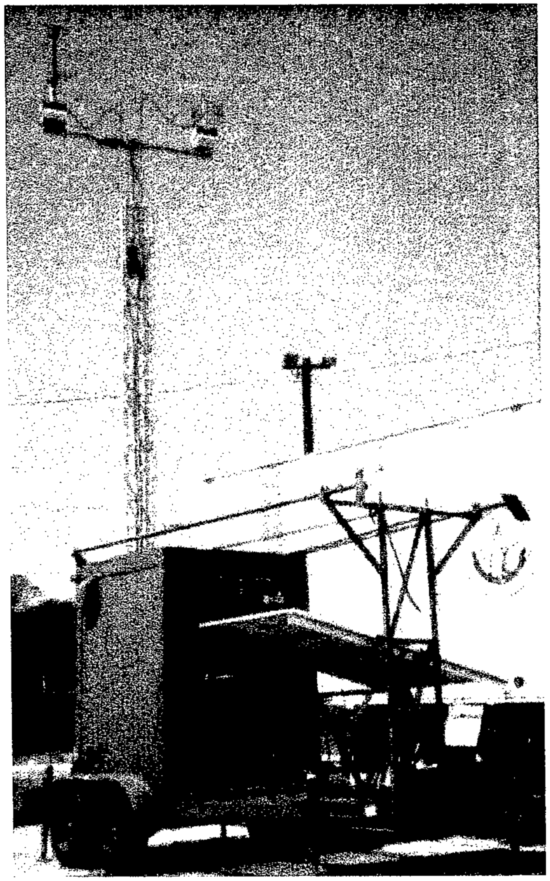
- SELF-CONTAINED SITE--CONCRETE PAD
- VARIABLE HEIGHT DEPENDING ON TERRAIN, VEGETATION AND OBSTRUCTIONS
- ALL WEATHER, DAY/NIGHT OPERATION
- SOLAR POWERED WITH BATTERY STORAGE
- LOCALLY ACCESSED WITH LAPTOP COMPUTER
- REMOTELY ACCESSED FROM COMMAND POST, MOBILE SENTRY OR PATROL VEHICLE
- TWO WAY COMMUNICATION
  - ◆ RADAR/VIDEO AND SELF-TEST DATA OUT
  - ◆ COMMANDS FOR SPECIAL REQUEST DATA IN



MOBILE UNIT

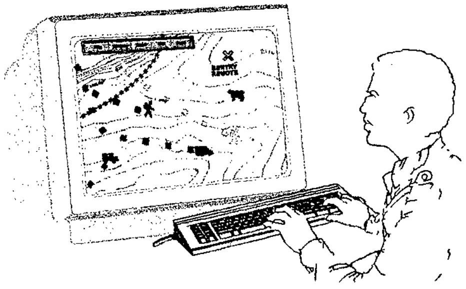


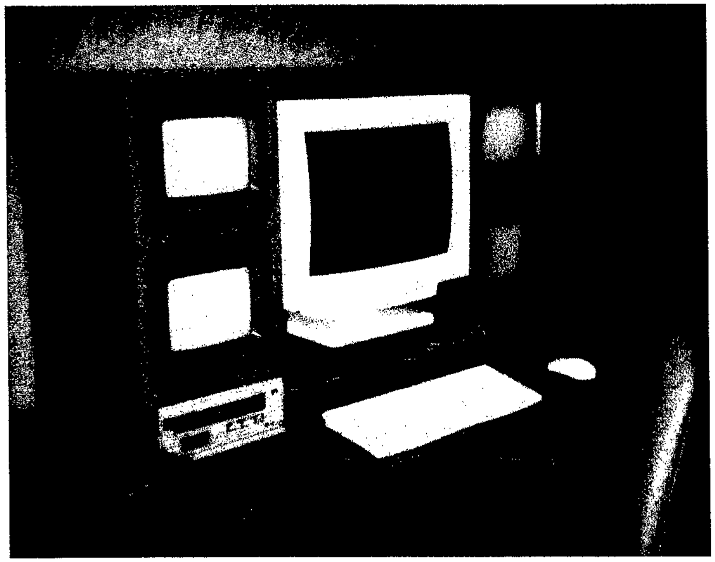
- CAN FUNCTION AS MANNED FIXED SITE OR MINI COMMAND POST
- CAN ACCESS ANY FIXED UNIT
- IMPROVES PERSONNEL SECURITY THROUGH SITUATIONAL AWARENESS
- MAST RETRACTS FOR TRAVEL
- COST GOAL - $50K PLUS VEHICLE



COMMAND POST

- AUTOMATIC COLLECTION / INTERPRETATION / PRESENTATION OF REMOTE SENSOR DATA
- GENERATES BOTH AREA OVERVIEW AND SITE-SPECIFIC DATA
- PRESENTS RADAR DATA ON AREA TOPOGRAPHY MAP
- PRESENTS VIDEO DATA FOR IDENTIFICATION
- OPERATOR CONTROL OF SITE AND DATA SELECTION AND PRESENTATION FORMAT
- SITE HEAVILY FILTERS DATA FOR REDUCED COMMAND POST MANPOWER





STS SENSOR TECHNOLOGIES & SYSTEMS, INC. COMARCO

RADAR SENSOR

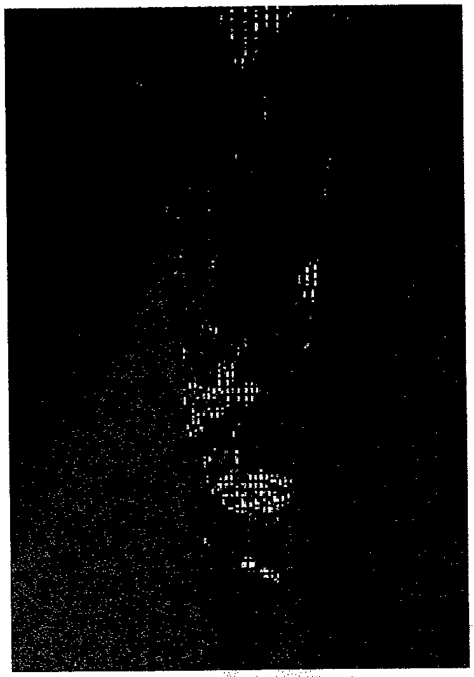
- DETECTS PERSONNEL, VEHICLES, LOW FLYING AIRCRAFT
- FMCW RADAR PROVIDES ADEQUATE PERFORMANCE AT LOW COST
- SEPARATE TRANSMIT AND RECEIVE ANTENNAS EXTENDS DETECTION RANGES
- LOW POWER - SAFE
- SPECIFICATIONS

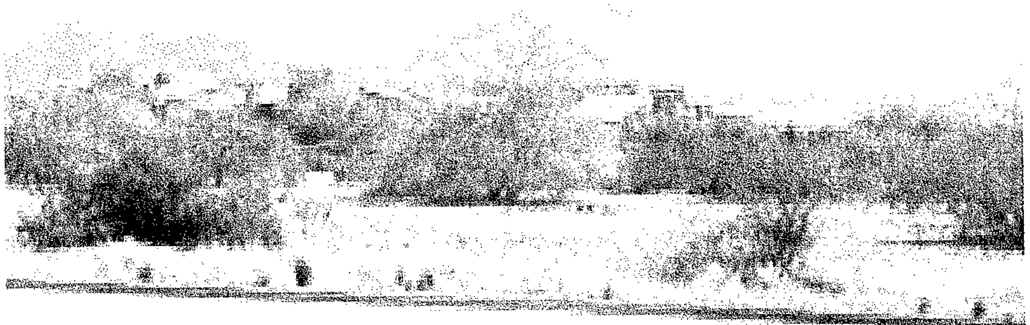
TARGET	
PERSONNEL (1/2m^2)	6.5 Km
JEEP (10m^2)	13.5 Km
TRUCK (100m^2)	24 Km
AIRCRAFT (10m^2)	13.5 Km
COVERAGE	
AZIMUTH	360 DEGREES OR SECTOR
ELEVATION	± 15 DEGREES
ANGULAR RESOLUTION	1.5 DEGREES
REVISIT TIME	10 SECONDS (FULL 360° SCAN)

SENSOR TECHNOLOGIES & SYSTEMS, INC.

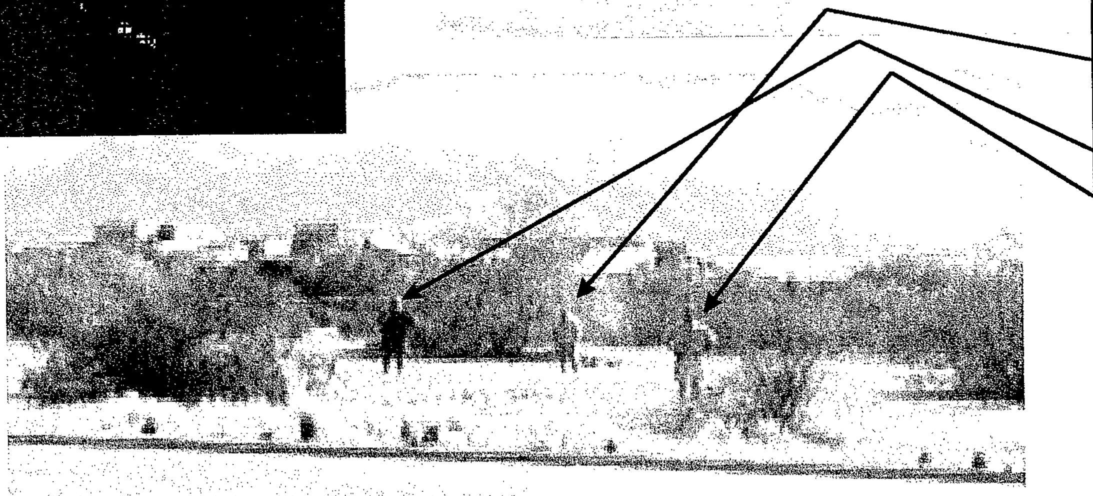
COMARCO

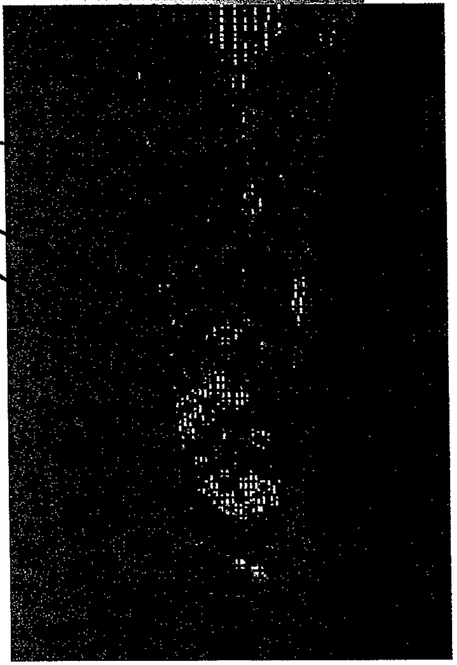
TYPICAL RADAR IMAGE





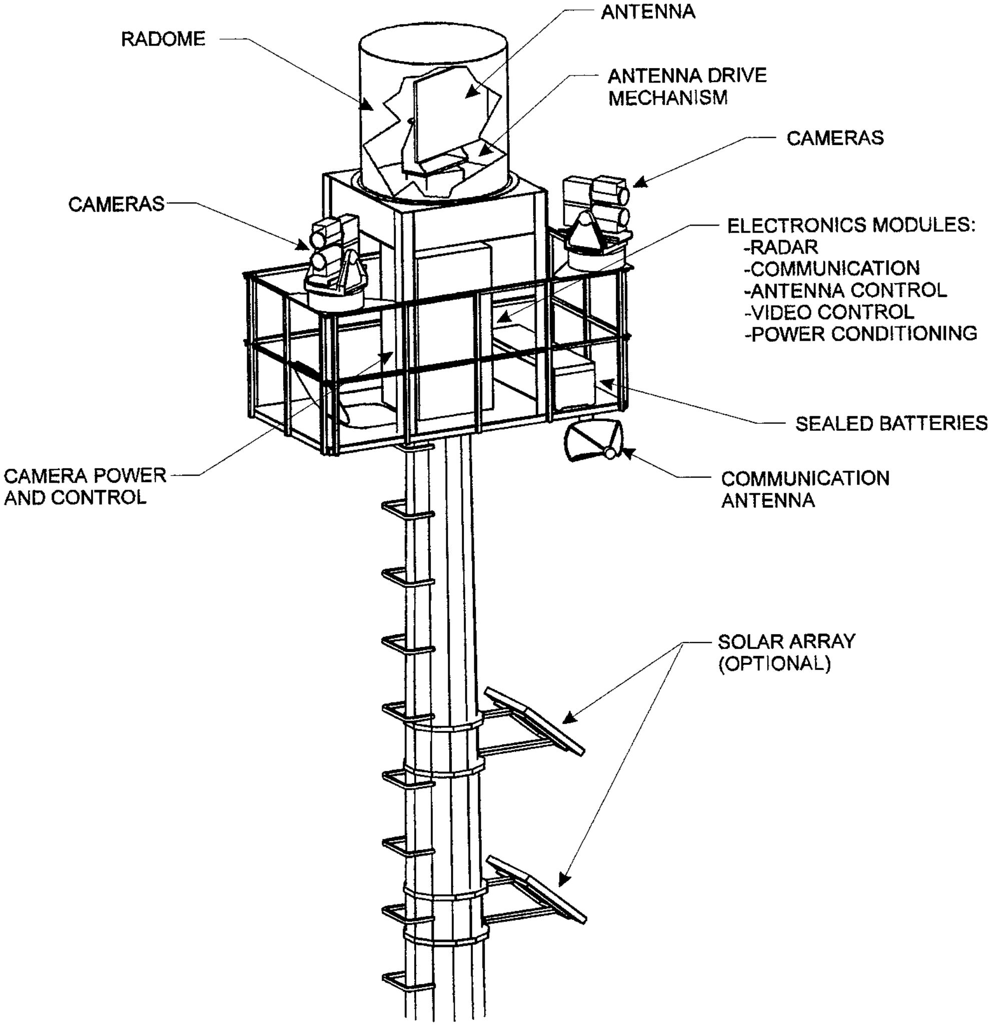
NO PERSONNEL PRESENT





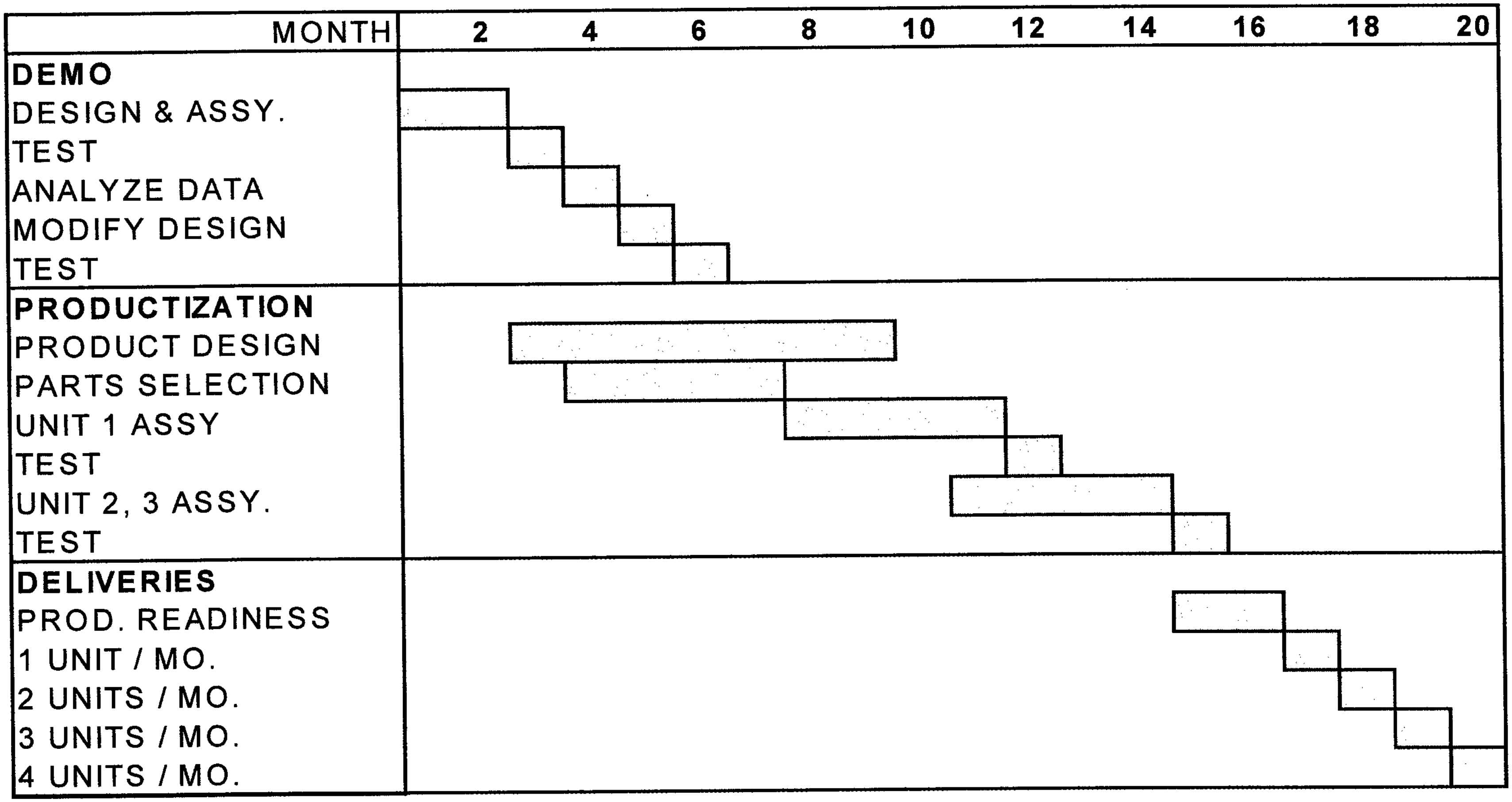
PERSONNEL PRESENT

STS SENSOR TECHNOLOGIES & SYSTEMS, INC. COMARCO



TYPICAL SENTRY INSTALLATION

SCHEDULE


MONTH
2
4
6
8
10
12
14
16
18
20
DEMO
DESIGN & ASSY.
TEST
ANALYZE DATA
MODIFY DESIGN
TEST
PRODUCTIZATION
PRODUCT DESIGN
PARTS SELECTION
UNIT 1 ASSY
TEST
UNIT 2, 3 ASSY.
TEST
DELIVERIES
PROD. READINESS
1 UNIT / MO.
2 UNITS / MO.
3 UNITS / MO.
4 UNITS / MO.

STS SENSOR TECHNOLOGIES & SYSTEMS, INC. COMARCO

OTHER APPLICATIONS OF SENTRY TECHNOLOGY

- FORCE PROTECTION
- SHORELINE / HARBOR SURVEILLANCE
- PRISON SURVEILLANCE
- MOBILE UNIT FOR INLAND SEARCH MISSION
- COMMERCIAL HIGH VALUE SITE PROTECTION

SUMMARY

- SENTRY PROVIDES HIGH RESOLUTION, LOW FALSE ALARM REMOTE SURVEILLANCE
- AUTOMATIC SENSING, MAN-IN-THE-LOOP RESPONSE DETECTION
- FLEXIBLE POINT SENSOR OR OVERLAPPING NETWORK
- FIXED AND MOBILE CONFIGURATIONS
- REDUCES SURVEILLANCE MANPOWER
- PROVIDES 24 HOUR, DAY/NIGHT, ALL WEATHER SITUATIONAL AWARENESS
- AFFORDABLE

"Helicopter Neutralization ---
Performance Testing Protective Forces"

Introduction

Many high risk facilities share a common threat of security incidents being perpetrated by adversaries utilizing rotary-winged aircraft. While the low numbers of actual helicopter-assisted security incidents worldwide suggest that such threats remain rare, the fact that they have occurred offers the obvious conclusion that they are indeed possible. In certain instances the consequences of a successful aircraft-assisted assault (in terms of danger to the public, national security, political damage and/or economic ramifications) are potentially serious enough that extraordinary measures may be justified to prevent such assaults from being successful. Examples might include raids targeting nuclear weapons facilities; military special/chemical munitions depots and naval magazines; or industrial facilities which are of strategic importance to the government of the country in which they are located. While no US Department of Energy or Department of Defense facilities to date have been targeted by adversaries attacking in helicopters, both US federal and state penitentiaries have experienced attempts to free inmates by confederates who have utilized or commandeered civil aviation helicopters. While escaping prisoners may not offer the same threat to the general public as the theft of plutonium or quantities of dangerous chemicals, seemingly innocuous facilities may offer threats beyond those initially recognized. For example, a high profile security incident perpetrated by animal rights activists against a facility utilizing animals to test pathogens or research cures for extremely virulent Eboli or Smallpox viruses may have far reaching consequences.

In most cases the range of potential adversary threats faced by these facilities is not changed significantly by the addition of helicopters. The use of helicopters by adversaries, however, can substantially reduce response times available to site protective forces. Because of the timeline advantages that helicopters offer to adversaries, it may be prudent to investigate the capability for helicopter denial demonstrated by your protective force as part of your annual sitewide security review.

This paper describes the development of performance testing which examined the ability of security forces to detect and neutralize helicopter threats. It describes the application of laser engagement simulation technology to provide data regarding protective force effectiveness. Guidelines and lessons-learned are presented which offer a means of replicating such testing at other facilities which may face helicopter threats.

Helicopter performance testing seeks to measure the relative capability of a protective force to deny adversary target access or escape by helicopter. Test outcomes express protective force capability to neutralize aircraft as ratios of "hits achieved relative to shots available", over time -- e.g. the findings are statistical values. These values thereafter may also be used in computer modeling processes.

"Helicopter Neutralization" • W.C. Brunsdon, CPP June 1998

While recognizing that Security Policy - e.g. 'identifying that point at which aircraft demonstrate "hostility" and may be engaged' - is also of critical importance, performance testing as described in this paper does not examine protective force actions in response to policy. Our focus examined *only* the tactical ability of the protective force to detect inbound aircraft and achieve a 90% probability of helicopter neutralization; and the technological means with which this might be measured.

PART I -- ESTABLISHING TEST DESIGN PARAMETERS

Threat Characterization

In most cases the first step when examining helicopter neutralization is to define which threats the site is defending against. The primary purpose of identifying which helicopter threats your site is defending against is to determine the probable duration and locations of aircraft exposure.

Helicopters possess certain operational requirements, which in many cases will point to certain "paths" to the target being more likely than others to be utilized by adversaries. Some of these include landing zone size requirements; wind and weather constraints; obstacles, wires, and other obstructions along an approach path; darkness and a need for ambient light at night in the vicinity of the objective; difficulty hovering over sand, dust, snow, and other environments which obscure visibility; and in some cases, short time on station - or time and range constraints based on the total weight they carry in terms of adversaries, the target being sought (if any), and fuel on board.

Different helicopters offer various performance capabilities, in terms of speed, rotor noise, and load capacity. Many potential environmental challenges can be overcome using technology - for example, attacking with helicopters at night by flying at nape-of-the-earth altitudes utilizing night vision goggles. Most aircraft performance characteristics are static, however: a given helicopter will only fly so far at top speed, and will only carry a maximum weight. This will limit and may help define adversary capabilities.

A survey of civil aviation helicopters for lease in your area will provide a range of aircraft performance characteristics which will assist in defining the "most plausible aircraft threat" you must protect against, based on aircraft availability and terrain/physical circumstances at or in the vicinity of your specific facility. [We made an assumption that adversaries are more likely to use an unarmed (i.e. non-weapons platform) civil aviation aircraft. This may not be the case worldwide.] Helicopters primarily provide a more rapid means of ingress or egress. All other attack actions in the objective area remain the same. Once on the ground, adversaries (and/or insiders) must defeat the same barriers and security measures to access the target that they would encounter without the use of a helicopter. Therefore, *in general*, your "worst case scenario(s)" as they are defined *without* the helicopter threat remain(s) your worst case scenario(s) *with* the helicopter threat, and for the same reasons - <u>they still offer the shortest path to the target(s)</u>. The addition of an aerial ingress/egress capability merely reduces response times available to protective force personnel.

There are several fundamental scenarios to be considered in planning helicopter interdiction tactics by protective force personnel; and subsequent testing of response behaviors. Specifically, helicopter-borne adversaries are most likely to do *one or more* of the following:

1) Pick up and escape with a target prestaged by insider(s) or other adversaries - i.e. no landing is required, but a brief hover may be required to attach target to a hoist (where it becomes an internal or external load);

2) Extract personnel/team - which requires a landing or hovering at a "near landing", while adversaries w/w/o target(s) run to the aircraft or secure themselves to rigging beneath the aircraft; and/or

3) Attack or provide diversions, etc. - adversaries may, for example, arrive via helicopter; deploy chemical agents, incendiaries, smoke, or conduct similar hostile actions from a helicopter, either individually or in support of other attacking elements on the ground.

As noted, the primary purpose of identifying which helicopter threats the site is defending against is to define the probable duration and locations of aircraft exposure during the adversary attack. Average attack exposure times might be, for example, 30 seconds to hover while loading; 20 seconds to load or unload personnel; and 10 seconds to ingress & flare/another 10 seconds to egress. Initially establishing a set of assumptions regarding aircraft exposure times is essential for test design. These assumptions can always be modified later, however, they are foundational for all follow-on tactical response planning; that is, they determine the length of time a protective force officer might have to acquire and engage the aircraft target. Hence, performance testing may determine the probable success provided by such planning. Often, aircraft exposure times may be derived using a variety of computer modeling programs and/or data provided by subject matter experts/consultants. Regardless of the source, it is necessary to determine which exposure times will be used before helicopter testing can be developed. Documenting how and on what basis these helicopter exposure times are established is critical. In order to obtain valid results the threat parameters must first be carefully defined.

Describe your current protection strategy against helicopter threats

The second set of performance test parameters which need to be defined are the protective force emergency response plans - the distances and angles at which attackers might be engaged with small arms; the number of shooters which logically might be expected to bring the aircraft under fire (within estimated time available); and other considerations which might impact either adversary or protective force behavior.

The tests we are describing cannot examine protective policies or defense strategies directly. Instead, the tests will allow determination to be made that - if the adversaries are exposed for a specific time; and if the protective force is able to bring X fire to bear on the adversaries during this time; then (a correlation against 'known values' suggests) there is a Y% probability that the adversary aircraft will be neutralized.

In turn, such values will allow computer modeling to take place which will indicate whether a protection strategy is likely to be successful, or the degree to which your strategy tends towards success or failure. Computer modeling also may provide other options. For example, using the assumed aircraft exposure times; modeling may suggest other response actions that are possible within the time limits available to protective force personnel. In reviewing your initial site protective strategy against aerial threats, consider factors such as:

- Your facility's physical qualities -- the presence of static barriers (e.g. fences, doors), natural terrain features, or other design characteristics which channel adversary movement or provide a tactical advantage to the protective force;

- Strategic response locations -- routes to these locations, likely target locations (in the air over rooftops, parking lots, etc.), obstructions to small arms fire against helicopters, and potential initial locations of responders at the moment of a random aerial attack;

- External resources -- military or police air assets, local radio station aircraft, local airports, etc. which might immediately provide visual assistance, radar tracking, or other response capabilities, etc.;

- Other factors -- terrain in the vicinity of the site, prevailing winds and weather patterns, glare lighting, etc.

The goal is to determine the probable number and locations of shooters able to bring fire to bear on adversary aircraft during an attack within the time durations identified. In addition to identifying test parameters (i.e. distances at which test aircraft will be engaged), this number also provides equipment and logistical requirements (i.e. MILES weapons, vehicles, radios, etc.) and personnel requirements, both Shooters/ Participants as well as Controllers, to support performance testing.

Create a written Statement of Test Purpose

A written statement defining the purpose of the performance test can be as simple as, for example, "...to determine whether or not current protective force resources are adequate to neutralize identified security threats". As with establishing the assumptions regarding threat parameters, it is critical to later determining the degree to which the test was successful, and the validity of the results; to define *specifically what we want to accomplish and how we intend to accomplish it.*

A written statement of the test purpose is crucial later when evaluating results because it provides a previously agreed upon standard or criteria against which to measure "what did we accomplish?"; or "to what degree were we successful - did we ultimately test what we wanted to test?". This in turn provides confidence that the results are either valid or are not valid, based on the degree to which they allow us to measure desired behaviors and/or outcomes.

The point is that post-test success or failure will be measured against previously identified purposes for the testing. In order to be "successful", then, the goals of testing must be rigorously constrained and defined. In the likely event that testing has not been done before, then no "pass" or "fail" should be determined. The goal initially is to simply establish a data baseline against which future test results can be compared.

PART II -- DEFINING LOGISTICS REQUIREMENTS

Identify sources for helicopter support services

Helicopter availability to meet your test requirements will, to a large extent, govern dates and times available for testing. Helicopter operations, as well as MILES weapons operation, are constrained by weather conditions. Otherwise, generally helicopter leasing companies will be able to meet your needs, but they must understand clearly what you want them to do. If your facility processes classified information or handles hazardous materials, classification issues may impact on your ability to communicate your needs to the commercial helicopter company. In this case, you should involve your Classification Office early in the process to avoid compromising classified information.

For the most part, commercial providers of helicopter services are willing to provide testing support, however, some may be able to do so with greater ability than others. We contracted with a company which provides both aerial camera platforms and stunt helicopters to the movie industry. Their pilots were used to hovering over buildings and moving vehicles, flight at unusual attitudes and maneuvers, being shot at with a variety of small arms or missiles, special effects, etc.

You must estimate the number of flight hours you need - i.e. hours in the air, not including hours on the ground getting personnel into position, etc. Demands for on-station airtime will drive fuel consumption and frequency of refueling stops, as will need to carry adversaries, targets, and other activities. You must be able to discuss in detail your requirements with the helicopter contractor in order to allow the contractor to plan for personnel, fuel and aircraft hours, however, as mentioned above, classification concerns must first be resolved. In particular, the attachment of MILES sensor harnesses to the exterior of the aircraft must be carefully understood by all parties. Care must be taken to provide for safety under all circumstances.

Pilots must be briefed that protective force personnel will be firing MILES weapons at the helicopter. Aircrew concerns must be discussed. Pilots should plan to be present at all pre-exercise briefings and observe procedures whereby participants are cleared of all live ammunition and weapons prior to MILES laser weapons and blank ammunition being distributed. You must provide weight estimates to the pilot for MILES harness & system controller/buffer, computer(s), technician and Helicopter Controller, videocameras, and other equipment needed in the aircraft. You may also want the pilot to wear a MILES harness, depending on the type of helicopter used.

A number of helicopter logistics requirements must be arranged among facility contractors or departments, and a team approach is suggested as the most efficient means of facilitating widespread communication and coordination. The following are basic requirements, others will be discovered throughout the planning process:

- A landing pad must be arranged, if none exists, and must be swept of gravel, dust, and small objects before the helicopter uses the pad.

- An emergency landing zone must be identified, such as a large open parking lot, lawn, or open area. It must also be examined for obstructions, trash, or small objects that could become airborne in rotor wash or could be sucked into engine air intakes.

- Write a Flight Safety Plan. Consult FAA regulations for flight in and around your facility. Your plan should be approved by safety engineers, in concert with building managers, shift supervisors, etc. What restrictions on aerial activity exist? Minimum altitudes? Environmental restrictions on flight? Site restrictions on flight (i.e. not over reactors)?

- Building managers and personnel must be notified if aerial activity is to take place over any building on your facility. Efforts should be made to schedule the test on a weekend, so that parking lots are clear and non-participant personnel in the area are minimized.

- Determine a safe location to conduct refueling of the aircraft. In many cases, the contractor will have a fuel truck they can position near the landing pad to facilitate quick refueling. This is invaluable during testing. Investigate fire department availability for hot refuel assistance/safety.

- Identify a location for the helicopter to report to in the event a real alarm or incident occurs during the test. This may be a small orbit above a predesignated ground location, to avoid delays if the interruption is not lengthy, or may mean landing at a local airfield or the primary landing pad to avoid incurring additional costs if the interruption is longer.

- Research availability of commercial airport services (tower, airspace control, refueling, emergency landing, etc.). Notify any local airport tower control of testing the day before. Are there radar and weather support services nearby which can quickly be contacted?

Identify sources for ESS/MILES weapons and equipment

Engagement Simulations System (ESS) or Advanced Multiple Integrated Laser Engagement System (MILES) equipment has been used by the military for over twenty years to simulate armed conflict between opposing forces. It is available through a variety of federal sources to government entities. It may also be available through a number of manufacturers to non-government entities, for either lease or purchase.

For the purposes of this paper, it will be assumed that readers are familiar with ESS/MILES laser weapons and equipment and the parameters concerning its use within the performance testing environment. A complete technical and operational discussion of the laser weapons and equipment is beyond the scope of this paper. Even assuming readers are familiar with ESS/MILES equipment, and may have used it in force on force exercises previously, readers must understand that such equipment is used much differently for gathering statistical data during helicopter neutralization performance testing than during standard force on force exercises.

It is important that you understand that, for the purposes of helicopter threat interdiction performance testing, there are significant technological differences between what is required of standard helicopter ESS/MILES equipment used during force against force exercises and requirements for ESS/MILES equipment needed to test helicopter neutralization. Equipment designed and set up for force on force exercises will NOT adequately support data gathering to measure anti-aircraft capabilities. ESS/MILES equipment is used during force on force exercises to determine whether ground-based small arms fire has "killed" or taken the aircraft out of play. Thus, the harness counts a random number of hits, often determined by a random number generator or preset before the exercise, and then activates - "killing" the helicopter.

This is counterproductive to the requirements of helicopter denial performance testing. During helicopter neutralization tests, the objective is to count the number of times the aircraft sustains hits from ground-based small arms fire over time. For example, results should indicate that within the first 10 seconds the helicopter was hit X number of times; within the second 10 seconds the helicopter was hit Y times; and within the third 10 seconds was hit Z times. This will yield a total number of hits over the total of 30 seconds, as well as hits per intervening intervals. To yield output of greater value, moreover, software should be utilized that tracks which specific laser weapon struck the sensors at which time, and in which chronological order. Advanced MILES weapons laser emitters are individually coded, and codes should be assigned to specific shooters/locations. Software times should also be correlated to exercise times - i.e. real time; so that ground actions/shooter locations may be judged in terms of one action or location being more valuable or efficient than another.

All data regarding MILES system performance should be capable of being recorded in a MILES system buffer, for downloading into a computer, either later or - ideally - as it occurs or "real-time". Analysis of data printouts will allow determination to be made of which firing position(s) produced the greatest number of hits, and total numbers of hits from specific weapons received over incremental aircraft exposure times. This type of data will also allow statistical conclusions to be reached regarding different probabilities of helicopter disablement under real world conditions.

We utilized an Advanced MILES system manufactured by Schwartz-Electro Optics (SEO), of Orlando, Florida. Known as the "Multiple Integrated Target System" or MITS, we understood that it would perform so as to meet our needs. Data stored in the buffer of the MITS system may be later downloaded into a computer hard drive.

The system provided a great deal of data, however, due to the differences between ordinary force on force exercise requirements and our requirements, it did not provide all the data we required. SEO technicians are currently exploring the potential for the system to be redesigned to more specifically meet our purposes.

One of the most important lessons learned during our helicopter performance testing was that the ESS/MILES gear must be carefully installed and must be functioning perfectly in order to gather all data and yield optimum results. Lack of sensors on the exterior of the aircraft; system delays in counting the number of hits received by the sensors, especially when multiple hits strike the sensor harness simultaneously; the inability of the system buffer to hold large numbers of hits; and system delays as the harness resets itself after "activating" (i.e. killing the helicopter); all negatively impact the validity of the data collected. [The data you recorded may be valid, however, questions remain regarding that amount of data you failed to record, and the relative percentages of data recorded to data lost.]

As a result of our experience it is recommended that you consider running your entire performance test first on the ground, on a preliminary basis, using a vehicle set up with the helicopter MILES harness, with all participants/shooters firing at the vehicle. This type of pretest run before the actual performance test is conducted with helicopters will provide cost-efficient experience to all participants and controllers, and offers a chance to ensure MILES equipment is working properly - providing a better chance at recording vital data later. Moreover, it provides experience to shooters at engaging targets moving at speeds of 30 to 40 miles per hour using MILES weapons (laser weapon ballistics are different from standard ammunition ballistics).

Another important lesson learned is that it is vital to have a technician from the manufacturer accompany the ESS/MILES equipment utilized. Equipment failures can have significant impacts on test success, and given the cost and coordination required to run the test, failures must be corrected rapidly (to the best of the technician's ability) so that the test is not cancelled. This requires skilled technical support.

Other lessons learned during Advanced MILES helicopter neutralization performance testing include:

- Ensure there are adequate sensors on outside of aircraft to record multiple simultaneous hits. In some cases, the MITS system buffer will only handle so many hits at once, in which case multiple buffers may be necessary, each with their own sensor harness. An alternative is to redesign system hardware to meet your specific requirements.

- Be aware of locations of sensors on aircraft relative to shooter locations on the ground. We utilized safety requirements that aircraft maintain 100' above ground level (AGL) - i.e. at times shooters were shooting UP at the bottom of the aircraft. MITS/Advanced MILES sensors were installed on step rails above aircraft skids on both sides of the fuselage, therefore, no hits aimed at the bottom of the aircraft would register on the sensors.

For any laser hit to be recorded, the angle of the laser beam to the sensor plane must be between 90° and 45°. Shots striking at an angle of less than 45° will not register on the sensor. Both vertical and horizontal sensor angles are impacted by this condition. Because no sensors were installed on the bottom of the helicopter, the laser to (side) sensor angle from distances approaching 50 yards for some shooters may have rendered many of their hits invalid. No sensors were installed on the front or back of the aircraft. Laser/shooter to (side) sensor angles for approaching and departing helicopters may have resulted in many shots which might have hit the aircraft under real-world conditions not being recorded by the MILES harness.

- Clarify requirements with the MILES manufacturer for data storage, retrieval, print-out for analysis, etc. This is critical to measuring results and outcomes. Be specific with the equipment manufacturer, in writing, as to what you expect the system to produce during the course of the performance testing. Examples include requirements such as:
  a) "we need the equipment to count the total number of hits received, over the number of seconds that the aircraft is exposed to fire";
  b) "we need a sufficient number of sensors and buffers so that all hits on aircraft vulnerable areas can be recorded";
  c) "we need all event times to be correlated to real-time";
  d) "we need individual weapons coded for later analysis as to which firing positions afforded the greatest number of hits, etc";
  e) "we need all data recorded to be printed out for analysis".

- Each time the MITS harness receives/records a hit, it shuts down for 1 second. No other hits can be recorded during this period, although the manufacturer indicates that by reducing the amount of coded data contained in each laser burst, this reset time may be significantly reduced (but not eliminated).

- Whenever the helicopter harness "activates", or indicates a kill, it shuts down and must reset - which requires a minimum of 4 seconds. After the system goes off and before it resets, no hits striking the harness will be recorded. [Ideally, helicopter sensor harnesses should not activate at all, but should simply count the number of times they are hit and by which laser transmitter.]

- Only one hit on a sensor harness at a time will be recorded. If two or more hits strike the harness simultaneously, only the first of these will be recorded. Computer printouts may indicate several coded weapons, indicating that multiple hits were being received, however, only one hit will be recorded - no count of all hits simultaneously striking the harness is possible.

- We used only two strips of 3 sensors each, instead of four strips. Only 5 sensors were available to be hit by ground fire. Even with so few sensors, the volume of fire received overwhelmed the system's ability to record hits. Even had we installed the other two sensor strings, and had shooter fire been accurate in striking these other sensors, no other hits could have been recorded by the control unit buffer - as it was already overwhelmed by the volume of fire striking the 5 sensors available. In the future, hardware redesign should reduce many of these concerns, however test plans must also be redesigned to accommodate the limitations of the equipment.

- The system was not designed to record heavy concentrated volumes of fire. The MITS buffer will only hold approximately 360 hits. Thereafter, until it has been downloaded, no further hits will be recorded. Hardware may be altered so as to raise buffer limits.

- Recorded events/data times were not correlated to real-world time. Each time the system reset, all system times were zeroed out again. System resets occurred frequently, due to operating the system beyond its designed parameters. Accordingly, printouts reveal numerous instances in which test times were zeroed out, resulting in a series of random time intervals. None of these intervals could be matched to specific times or event during the test; thus no correlation of "X hits received during 20 seconds", etc. could be derived.

- Be aware that additional ground-based testing may be required to substantiate Advanced MILES/MITS findings. For example, for protective force personnel equipped with fully automatic or "burst-capable" weapons, the laser transmitter will only emit 'one laser pulse per trigger pull'. The first blank round actuates the laser pulse. Only one pulse will be transmitted, regardless of how many blanks are fired. Therefore, the aircraft harness will only register one hit, assuming the pulse strikes it.

  This suggests that, if multiple projectiles are fired in short bursts by protective force personnel; in order to obtain credit for multiple hits on the aircraft, additional testing must be performed on the live fire range to document the capability of shooters to hit aircraft-sized targets at various ranges with multiple projectiles fired in short bursts. Thereafter, a 'force multiplier' value may be applied to total harness hits which will account for multiple projectiles striking the aircraft with each single laser pulse recorded.

We were using the Advanced MILES system beyond its designed operating parameters. The lesson is that tests must be designed to take the limitations of technology into consideration, and technological design limitations must be well understood, to acquire optimal data. Currently, it remains unknown whether any off-the-shelf technology exists, to allow this specific type of anti-aircraft testing to continue. SEO is currently examining both hardware and software to design a more responsive MITS helicopter neutralization testing system.

Global Positioning System (GPS) equipment and software

Standard civilian GPS units were used to identify helicopter locations and distances from site when the aircraft was initially spotted. First, initial locations of protective force posts were entered into the units. During testing, as the aircraft approached the facility, aircraft locations when the protective force first reported the aircraft inbound were also programmed into the GPS devices. Distances were then calculated by the GPS units between the location at which the aircraft was spotted, and the location of the post which spotted it. This information was downloaded from the GPS units themselves into computers, and commercially available software was then used to generate maps illustrating the relative protective force positions and aircraft locations as each test attack took place. The period between the time at which the aircraft was spotted and the time it arrived over the target area was recorded using stopwatches. These approximate intervals could be used to estimate reaction times available to protective force personnel.

Over time, and with repetition, such data yields graphic representations of likely helicopter avenues of approach; probable locations where it would likely be spotted; and approximate response times available to protective force personnel in which to react. You may discover that at your facilities, some of your resulting reaction times may be less than expected, which may impact on your tactical response and weapons or equipment planning. The following steps were taken to establish this capability with commercially available Global Positioning System hardware and software:

1) Survey GPS equipment available currently; features which facilitate data gathering; and related computer software which allows linkage with GPS units, data downloading, and subsequent analysis; and

2) Practice downloading coordinates acquired during pre-testing into software, and using software to generate maps, distances, etc.

Camera's: Documentation with Video and Still Photography

Photographs and videotape documentation provide a significantly greater, more in-depth explanative ability for clarification of problems encountered; test circumstances and environmental influences; and foundations for analysis and post-test problem-solving. We used one videocamera and one still digital camera to record data and to document test conditions. Both provided a vital sense of test conditions, difficulties encountered on the firing line, and angles of visual observation and fields of fire. More may be used, depending on your individual circumstances. During the data analysis phase, still digital photos were scanned into a computer and printed with a color printer, so that images could be imported into final reports provided to management.

Personnel

Pre-test training is of tremendous importance. This does not refer to job oriented training, which should already be accomplished, but to pretraining for running helicopter detection and neutralization performance testing. Consider the following:

- Shooters should receive instruction in MILES equipment stoppages and weapons failure drills, which may occur more often than encountered when firing standard weapons. This is critical for achieving maximum MILES hits on the helicopter within very short time durations.

- Two shooting relays were used so that one relay could be reloading while the other was firing, thus reducing aircraft downtime. Controllers should receive training regarding shooting line safety and the manner in which shooting relays are to be moved from location to location during the tests. A dry run or pre-test using a vehicle would be of value to rehearse both participants and controllers.

- Videocamera Operators and Photographers should receive instruction regarding camera angles sought to document helicopter engagements. In particular, documentation showing shooter positions and views of the helicopter from each shooter's location are useful during later analysis.

Pre Test Planning

A team approach was used to ensure cross departmental communications and coordination. "Punch-List meetings" were held twice weekly, at which all logistics coordination planning efforts were tracked, problems identified and responsible parties identified to resolve issues. At each meeting, events were systematically confirmed as completed and the integration of future support efforts was planned. These meetings proved critical to the success of the overall endeavor. Several items were specifically discovered to be especially important.

In particular, administrative procedures must be approved for passing out/retrieving MILES weapons and ammunition, and ensuring separation of live ammunition/weapons from MILES ammunition/weapons; if such procedures are not already in place.

A comprehensive understanding of the overall intent must be well communicated. In our helicopter neutralization performance testing we initially sought to establish average baseline "hit ratios" for individual shooters, firing at a helicopter from known distances, for predetermined exposure times. This information was general enough that it could later be input into different computer modeling software and applied to multiple scenarios. Ensuring this was well understood by all personnel paid off later, when Controllers reported numbers of rounds *unfired* from malfunctioning magazines and other essential data which had not previously been considered.

Rangefinders and orange cones were used to mark the individual firing positions and known distance "firing lines" used to establish statistical probability of hits at various distances (from each helicopter "target"). We discovered that a central firing line controller, located in an elevated position and equipped with a bullhorn, was extremely useful to control the widely distributed firing lines. Firing lines were established at 50, 100 and 200 yard distances from helicopter targets. Only one firing line was active at a time, beginning with the 50 yard line. Shooters stationed along each firing line were divided into two relays - port and starboard - so that half the shooters were firing while the other half were reloading.

As each shooter began each iteration of the test with a full duty load of ammunition, this meant that each shooter generally fired a full duty load during each iteration, and had to reload in between each iteration. Time constraints dictated that 2 relays per firing line were the most efficient use of helicopter flight time. Each relay at each firing line engaged the helicopter three times, to achieve a statistical average of hits at each line. Each firing line was thus run six times, three times for each relay.

Arrangements must be coordinated for logistics support during testing. Helicopter time is expensive, and there is a need to be able to solve problems encountered during testing rapidly so as make efficient use of the aircraft. In particular, a tremendous amount of blank ammunition will be fired by shooters. MILES weapons and magazine failures should be expected, and preparations made to replace weapons and magazines as they fail, or clean or repair them. Attention must be paid to details. Armorers should be available with spare weapons, tools and lubricants.

Written permission should be obtained from building managers over whose buildings the aircraft will be hovering, due to potential impact on air conditioning systems, communications equipment, and other rooftop mounted building control systems.

Emergency Responder Notifications

Aside from the notifications made administratively to impacted organizations, management, and surrounding authorities; identify those agencies and resources you would need to communicate with in the event that any real-world emergency should take place while testing is being conducted. A minimum list of such "mutual aid" responders might include examples such as:

- Medical Response (ambulance);
- Fire Department;
- Local Law Enforcement Agencies;
- Electrical Utilities, Mutual Aid Resources, etc.;
- Tower Control at Local Airfields;

In particular, arrangements should be made to have fire apparatus standing by when the helicopter lands, and during all hot refueling operations. This allows the helicopter to rapidly be refueled on the landing pad in between performance test iterations.

PART III -- CONDUCT OF TESTING

Establishment of Flight Safety Parameters

Flight safety parameters include both primary and emergency landing pads, possibly temporarily arranging for use of a large parking lot; and a helicopter landing zone for in-flight emergencies. These areas must be swept for debris or "foreign objects on the deck" ("FOD"), and carefully examined for obstructions or environmental factors such as blowing dust, snow, etc.

Flight safety plans must be reviewed by Safety Departments, must identify all high obstructions in and around your facility, and should conform to all safe FAA standards. In particular, Flight Safety Plans must be gone over in detail with the helicopter leasing company and the pilot, so that all personnel involved are aware of safety considerations.

Laying Out and Controlling Firing Lines and Shooting Positions

Individual shooting positions and general line configurations must be established the day before the performance test, after the parking lots have emptied out. Establish the location of the Central Line Controller at center of firing lines, equipped with a bullhorn and radio to call cease-fires as needed, to best control movement of test participants on the ground. The Central Line Controller must also be in contact with the Helicopter controller. Controllers with at individual shooter positions or vehicles containing two shooters will control staged firing and movement, ammunition reloading, problems related to MILES weapons, location of photographers relative to shooters, etc. Ensure that arrangements are made to collect all spent brass at the conclusion of the exercise. Ensure the Armorer is stationed in the vicinity of the firing lines, where shooters can take MILES weapons for lubrication, brief cleaning, etc.

Contingency Plans for Actual Emergencies

Contingency Plans must be established and reviewed by all Controllers for execution as needed during the limited scope performance test. Contingency Plans include, but are not limited to, such interruptions as:

- Actual Alarms and Incidents, and subsequent activation of actual (non-test participant) protective force personnel in response to the Alarms;
- Weather Interruptions;
- Illness (during our testing one shooter had to withdraw from the firing line due to illness);
- Non-reparable Equipment Malfunctions;

In particular, if protective force personnel are utilized as performance test shooters and are armed with MILES weapons; specific and detailed contingency plans must be prepared and briefed which set forth the manner in which -- during response to an actual alarm occurring during the performance test -- MILES-armed shooters and Controllers will cease all activity while the "Shadow Force" (actual protective force personnel armed with real weapons) responds to the incident and/or clears the alarm.

PART IV -- ANALYSIS OF FINDINGS

Data Collection Sheets

Data collection packets were distributed to Controllers during the pre-exercise briefings. They contain forms that Controllers are to fill out regarding data the Analysts need to corroborate MILES buffer printouts, GPS data, and stopwatch response times from the helicopter controller. At the conclusion of the exercise, the Senior Controller must collect all data collection packets from all Controllers. These must be locked up together with any computer print-outs; videotapes; photographs; and any other identification of test results. Your raw data may require classification.

Data should be reviewed by a team of analysts who will establish preliminary findings and outcomes from all raw data. The goal is to arrange hits over time in matrices which set forth the relationship between aircraft exposure time and the probable number of hits sustained by the aircraft during different exposure times; as well as which shooter locations afforded - in general - the most favorable conditions under which to engage the aircraft. In our case, outcomes included both total hits received by the system at varying ranges and exposure times, as well as findings regarding shooter location efficiency and other ideas for enhanced training. Additionally, aircraft GPS locations and distances should be examined to refine any anticipated aircraft ingress/egress routes, and potential actions to be taken in response to findings.

Correlation of Findings

Data regarding number of hits over time and probable neutralization outcomes, should be correlated using known statistical performance parameters. Information may be found in both US government and private references providing baseline helicopter neutralization data. We utilized baseline data taken from a classified report produced by the US Army's Piccatinny Arsenal (Rahe & Chu 1997), and from Gene Greneker (1991) of Georgia Tech Research Institute. Beware of bias injected during performance test design, which may influence both data gathering as well as findings.

Application of Results/Findings to Current Protection Strategy

Results should be analyzed with your protection strategy against helicopter threats, as defined during your initial performance test planning stage. Subsequent computer modeling using this data should provide at least preliminary indications that the strategy is either possible, or is not possible given current resources and plans. Remember that all findings are essentially baseline, and that results should be corroborated by additional testing prior to significant changes being implemented. Alterations to site protection strategy, emergency response plans, training, shooter positions, etc. should be contemplated as part of an integrated response planning function.

Outcomes Analysis -- "What does it all mean"?

Remember that different individuals may review the data and arrive at different conclusions. You may experience a situation where someone attempts to take your findings and apply them to a slightly different set of circumstances. This can be misleading. This is the point at which test results must be carefully scrutinized in view of the initial purpose and goals of the test; and outcomes must be strictly constrained by those parameters established early in the process. Just because X number of hits were sustained by a helicopter hovering for Y seconds, for example, it cannot be extrapolated that Z number of adversaries jumping from that helicopter would sustain any measurable reduction in offensive capability. All performance test outcomes must be strictly interpreted in light *only* of the original test conditions.

The data resulting from the test must be analyzed only against the pre-identified standards and criteria for Protective Force behaviors. Findings must be compared only against previously declared intentions. Questions regarding the validity of the data already exist due to artificialities invariably introduced during the performance testing process. It would be unhelpful to attempt to 'what if' the outcomes, and draw conclusions regarding other, more broad scenarios from the data derived from very constrained scenarios.

Your analysis seeks to confirm the answer to the question "did we ultimately wind up testing what we wanted to test"? This requires a careful review of findings against the initial statement of assumptions; as well as subject matter expertise, good judgement, and common sense.

Recommendations

It is the responsibility of the team of analysts to draw logical conclusions from the test findings and outcomes. They seek to answer the question: "Where do we go from here"? They seek also to recommend different options for the protective force and security management to enhance the facility strategic planning against helicopter threats. Be careful with your recommendations!

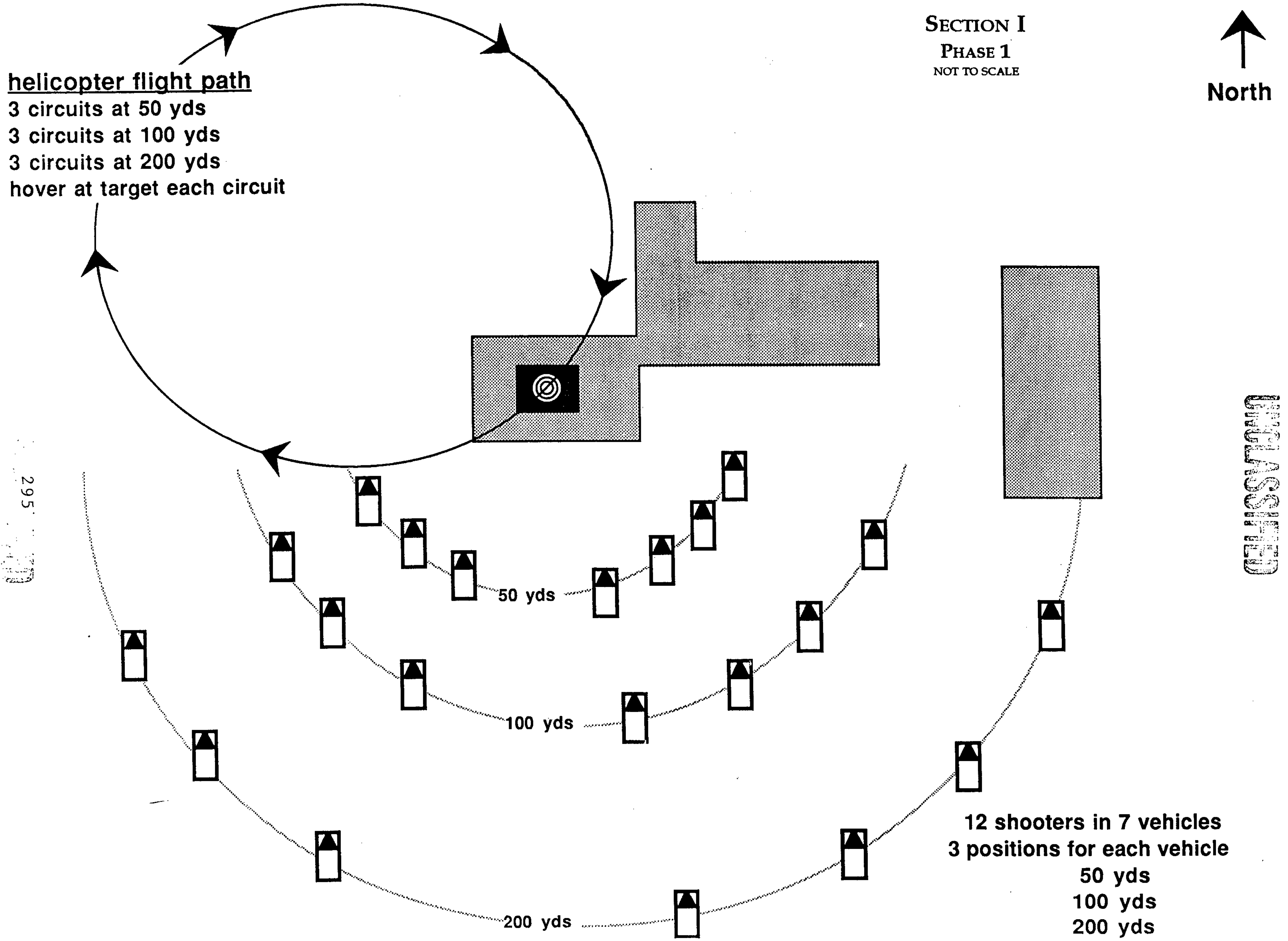
It is important to avoid pitfalls while drawing conclusions from data derived through highly-constrained test parameters. Many pitfalls involve assumptions that the results of the performance test truly represent reality; i.e. that the results are valid. It is important to remember that *any initial results take the form of unproven hypotheses*, and require additional performance testing before they can either be confirmed or be dismissed as misleading.

SUMMARY

This paper described lessons learned during the design and development of performance testing which examined the ability of security forces to detect and neutralize helicopter-borne adversary threats. We have reviewed the significant definition of goals and coordination required to conduct such testing, as well as the difficulties involved with attempting to derive meaningful results from tests conducted under obviously artificial environmental conditions and numerous safety constraints. For additional information please contact:

William Brunsdon, CPP
Wackenhut Services, LLC., Rocky Flats Environmental Technology Site
P. O. Box 464, Building 441, Room 106-6
Golden, Colorado 80402-0464
Phone (303) 966-8242 Email: wbrunsdo@du.edu

UNCLASSIFIED



SECTION I
PHASE 1
NOT TO SCALE

PHOTOGRAPH CAPTION ROSTER --

#1 "Closeup of Advanced MILES sensor attached to steprail located just above the helicopter skids on each side of the aircraft."

#2 "Port view of aircraft with complete sensor strip attached to the steprail. Note wire disappearing into the passenger compartment off the aft end of the steprail."

#3 "Advanced MILES System Controller for the Mobile Independent Target System (MITS). Equipment provided by Schwartz Electro-Optics, Inc. of Orlando, Florida."

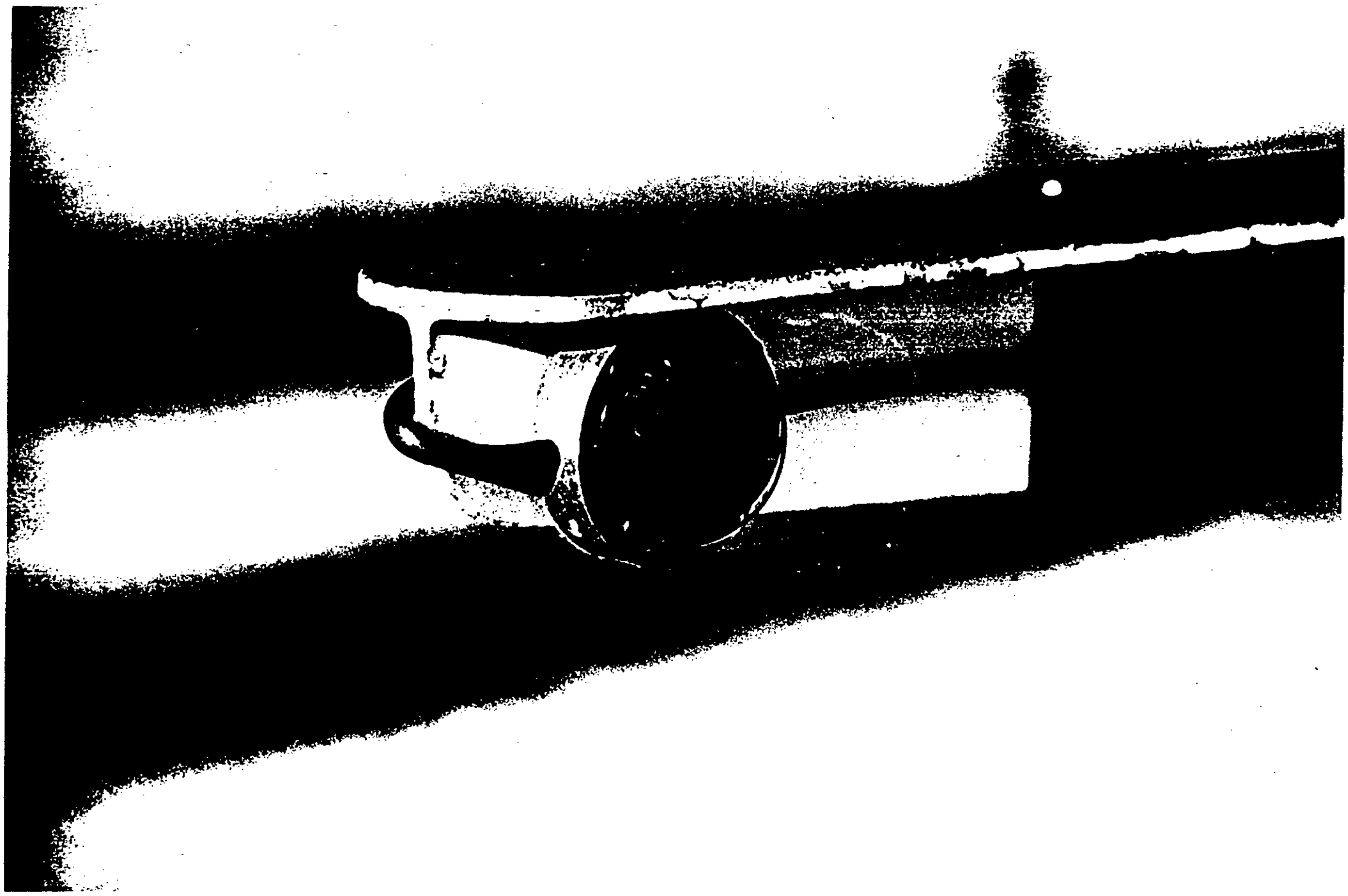
#4 "Security Police Officer firing at helicopter as it settles into a hover over the top of a building. Range is approximately 50 yards."

#5 "Helicopter simulates the pickup of an assault team escaping with some type of target by hovering over a building for a period of time, while being engaged by Security Police Officers. Range here is approximately 50 yards. The helicopter must hover at a higher altitude above ground level than might be the case otherwise, for safety purposes. Note the Exercise Controller at the front of the security vehicle, and the videocamera photographer recording shooter activity."

#6 "Security Police Officers utilized improvised supported shooting positions while rapidly acquiring their targets from vehicles. Note that this female SPO is firing from an offhand position with the forearm of the weapon supported from the bottom of the window while the vehicle door is open."

#7 "At longer ranges shooters found that they obtained better results by dismounting from vehicles and assuming different hasty shooting positions. Note orange cones identifying shooting line distances, and Safety Controllers with each security vehicle."

#8 "A helicopter assisted security incident could occur at a wide variety of facilites which offer critical assets. Does your protective strategy or emergency response plan currently provide for this type of planning?"



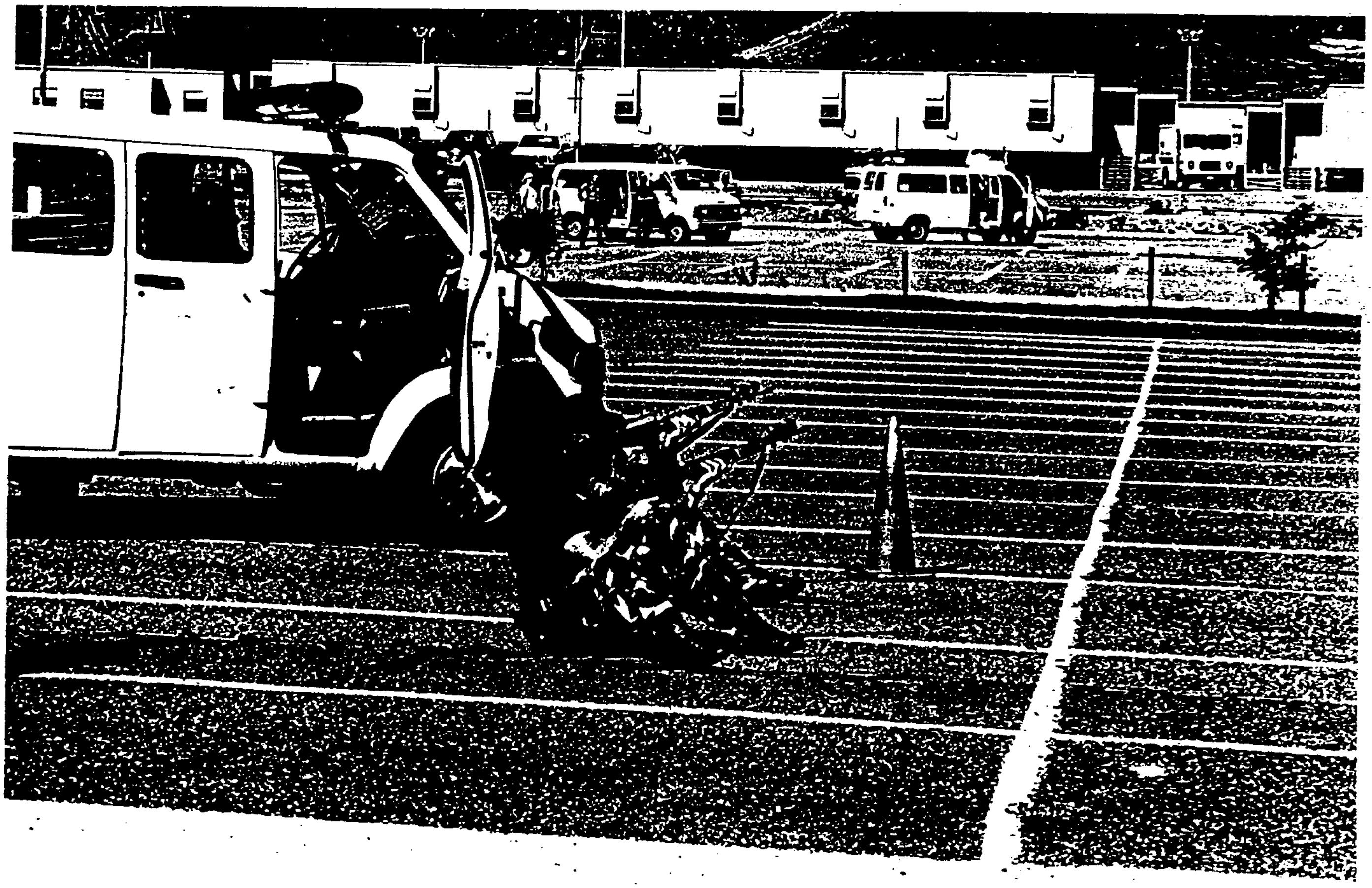
206BD

UNCLASSIFIED

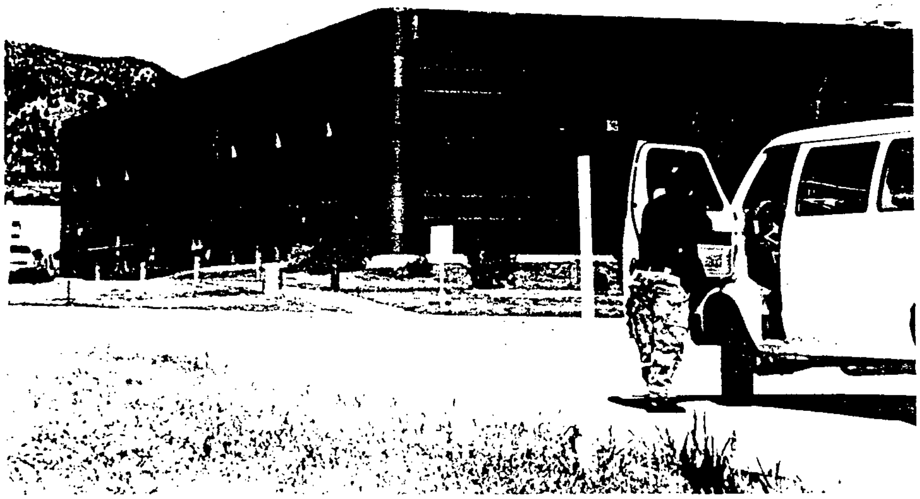
#3

58

#6



#7



U.S. AIR FORCE LASER ILLUMINATORS

By:

Dean S. Adler
Horizons Technology, Inc.
Billerica, MA

Supporting

Force Protection C2 SPO
ESC/FD
Hanscom AFB, MA
781/377-8393
DSN 478-8393
E-mail: adlerd@hanscom.af.mil

June 15 – 18, 1998

NDIA 14th Annual Security Technology Symposium
Williamsburg, VA

U.S. AIR FORCE LASER ILLUMINATORS

Dean S. Adler
Horizons Technology, Inc.
Billerica, Massachusetts 01821-4196

ABSTRACT

The US Air Force is pursuing the development of tactical laser illuminators to be employed by USAF Security Forces in the protection of high-valued assets. Through the effects of illumination, glare, and psychological impact, lasers can provide unequivocal warning, threat assessment based on reaction to the warning, hesitation, distraction, and reductions in combat and functional effectiveness. Two developmental programs are described, including hardware descriptions and Air Force plans for future activities.

LASERS AS TACTICAL ILLUMINATORS

In the present domestic and world political climates, military and law enforcement forces are faced with a growing number of situations in which non-lethal response options are essential. Recent examples include Somalia, Cuban refugee camps, Haiti, Saudi Arabia, and Panama, as well as the riots in Los Angeles and thousands of daily encounters that endanger police officers and bystanders. In these situations, the individual soldier or police officer would benefit from non-lethal options to warn, deter, delay, or incapacitate an adversary. Tactical laser illuminators help to "fill in" gaps in the force continuum between the extremes of verbal challenge and lethal force.

1. What tactical advantages can laser illuminators provide?

Low power (100 – 500 mw) laser illuminators used in a defensive role can induce the effects of illumination, glare, flashblinding, hesitancy via psychological impact, and reductions in combat and functional effectiveness of potential adversaries. These effects are all purposefully intended and proven to be entirely reversible, i.e., no permanent injury is likely to result based upon approved rules-of-engagement. Furthermore, if continuous-wave lasers are employed rather than "pulsed" alternatives, these effects are achieved at exposure levels far below the maximum power allowed by internationally accepted safety standards. Such laser illuminator devices can provide the system operator a unique array of non-lethal response options that can be increased in severity as the situation warrants. These options are:

- **Unequivocal, Language-Independent Warning** – A 1 to 2 foot diameter spot of bright red light illuminating the adversary's torso makes it clear he has been detected, singled-out, and likely has lethal weapons trained on him.

- **Threat Assessment Based on Reaction to Warning** – The intent/motivation of the adversary and the need for a more severe response can be assessed based upon whether the threat surrenders retreats, continues to advance, or raises a weapon in response to the warning. Quick conversion to a lethal response is assumed.

- **Slowing or Stopping the Advance of Individuals Through Temporary Visual Jamming** – Laser "dazzle", glare and flashblinding make it difficult to see a path, road, or obstacles, especially at night.

- **Impairing an Adversary's Ability to See in the General Direction of the Laser Illuminator** – Adversaries looking towards the laser source can see little or no detail about the location and placement of opposing forces.

- **Interfering With an Adversary's Ability to Accurately Aim a Weapon to Return Counter-fire** – Weapon firing accuracy is severely degraded by laser glare.

These tactical laser illuminators can be helpful in delaying and/or disorienting adversaries where innocent bystanders are present, such as hostage rescue, protection of political leaders or military commanders, and flight-line security. Finally, civilian law enforcement applications, such as drug raids and hostage rescues, where a second or two of distraction, fear, or visual impairment can provide the tactical edge needed for a successful engagement.

2. Saber 203

US Air Force Security Forces have documented operational requirements for a rifle-mounted, glare-producing, anti-personnel laser illuminator intended to provided security forces with additional engagement options when encountering adversaries. The integral M-16/M-203 weapon is selected to allow a laser illuminator round (IU) in the form factor of a 40 mm grenade to be loaded into the M-203 grenade launcher tube in place of a high-explosive munition. A separate Triggering Transmitter Unit (TTU) easily fastens to the launcher tube and houses the activation button and "AA" batteries used to power Saber 203. The system operator can illuminate, induce glare, and delay/disorient intruders using the Saber 203 non-lethal laser capability. If the situation escalates and warrants lethal firepower, the operator can fire lethal rounds immediately using the M-16 rifle. Red laser light was selected to provide an unequivocal, language-independent warning irrespective of cultures encountered when deploying worldwide.

Under development at the Electronic Systems Center, Force Protection C2 SPO, Hanscom AFB, MA, Saber 203 is currently completing a two-year Engineering and Manufacturing Development (EMD). The primary objectives of the EMD program are 1) improve the earlier design while managing eye safety to avoid laser eye injuries; 2) ruggedize system hardware consistent with world-wide deployments; and 3) reduce manufacturing costs consistent with moderate production rates. To meet these goals, design improvements have been accomplished in the areas of beam quality, operating temperature range, electronic drive circuits, and environmental sealing.

Specific design challenges have been to accommodate three subsystem modules within the compact volume of a grenade shell, i.e. within 40 millimeters in diameter by 132 millimeters in length. Modules included are:

- an electronics module with four printed circuit boards;
- a laser module, containing a solid-state diode laser with coiled fiber-optic (used to "homogenize" the beam in order to eliminate localized "hot spots" of output beam intensity);
- an optics module to "spread" the beam in order to achieve the desired "footprint" of laser energy at tactical ranges.

Qualification Test and Evaluation (QT&E) was conducted to validate prototype hardware against the system specification. In August 1998, AFOTEC, the Air Force Operational Test and Evaluation Center will conduct Initial Operational Test and Evaluation (IOT&E) at Kirtland AFB, NM to assess Saber 203's operational effectiveness in real tactical environments. Upon successful testing, AF Security Forces are planning on "trial" deployments for the remainder of the calendar year.

3. HALT

HALT (Hindering Adversaries with Less-than-lethal Technology) is a Saber 203 product improvement under the Air Force "spiral development" philosophy. HALT will accomplish improvements in three areas:

1) Totally eye-safe at the aperture. (Saber 203, by contrast, is eye-safe at ranges in excess of six meters);
2) Design for compatibility with the universal rifle mount and the future Modular Weapon System, allowing operation on most rifles in the U.S. inventory;
3) Capable of autonomous, hand-held operation - - no rifle required. Law enforcement can use as augmentation to sidearm.

HALT, like Saber 203, will allow the illumination of threats with intense (yet eye-safe) red laser light. Activation results in continuous-wave illumination that reverts to a "flicker mode" after ten seconds in order to maximize annoyance and disorientation of the adversary. In addition, HALT will effectively glare at considerably longer ranges than Saber 203 in both day and night conditions and will provide area illumination at a standoff distance of approximately one-kilometer.

Under development at the Air Force Electronic Systems Center, Force Protection C2 SPO, Hanscom AFB, MA, HALT is currently in a Technology Demonstration phase which is planned to be followed by an Engineering and Manufacturing Development (EMD) program in Fiscal Year 1999. The HALT EMD program will culminate in sixteen months with operational testing to assess tactical effectiveness. Production start-up is envisioned in Fiscal Year 2001.

4. Laser Eye Safety Bio-Effects Studies

Non-lethal weapons for employment in anti-personnel roles require thorough medical and legal study before proceeding to production and deployment. Saber 203 and HALT are not exceptions. Medically speaking, the first question asked by potential military and law enforcement personnel concerns eye safety. Both Saber 203 and HALT are designed to be "eye safe" in the sense that the laser output beam intensity at operational ranges is below the Maximum Permissible Exposure (MPE) - - the safety limit set by U.S. and international standards. These laser illuminators are:

- "Safe" for up to a 10-second exposure
- As "safe" as looking at the sun for longer exposures
- About 10% of the exposure levels produced by some laser pointer and laser firearm sights.

Unfortunately, this is not the whole story. Laser eye damage is not a binary process (no injury below the MPE, definite injury above the MPE), but rather a probabilistic process. The MPE is derived by finding the exposure level (based on intensity, emission wavelength, beam divergence, pulse characteristics, etc.) where 50% of exposures result in minimal permanent injury, then dividing by ten to get the MPE. There is still some probability that an exposure below the MPE will cause an eye injury in any given event - - no one knows, but it is small! The work necessary to fully define the probability of eye damage for all possible values of the aforementioned variables is far too extensive and expensive. Furthermore, the MPE is defined for unintentional exposures, not for intentional exposures like those produced by non-lethal weapons. How is this dilemma to be resolved?

In 1996, the Department of Defense published DoD Directive 3000.3, Policy for Non-Lethal Weapons. The policy states "Non-lethal weapons shall not be required to have a zero probability of producing fatal or permanent injuries. However, while complete avoidance of these effects is not guaranteed or expected, when properly employed, non-lethal weapons should significantly reduce them as compared to physically destroying the same target."

With respect to the Saber 203 program, specifically, funding has been provided to Air Force Research Laboratory – Brooks Air Force Base, to conduct analyses and measurements to accurately determine damage thresholds indicative of permanent injury. The exhaustive efforts at Brooks AFB resulted recently in the Air Force Surgeon General's Office approving Saber 203 for human use testing. Similar investigations are planned for the HALT program.

5. Formal Legal Reviews

Any new weapon, lethal or non-lethal, irrespective of the level of complexity or simplicity, is required by policy to undergo a thorough legal review prior to fielding. Saber 203 and HALT are no exceptions. Each program will be extensively studied by the OSD General Counsel to assure that each non-lethal laser illuminator complies with both the International Laws of Warfare and Compliance with Treaties. This review will occur in earnest once operational testing is completed on each system.

6. Summary

Tactical Laser Illuminators, including Saber 203 and HALT, are intended to provide field commanders and security forces personnel with additional options when engaged in peacekeeping and/or humanitarian missions. With other non-lethal alternative solutions, Saber 203 and HALT help to fill in "gaps" in the force continuum between a verbal challenge on the one extreme and application of lethal force on the other.

Air Force laser illuminators are intended to impart strong messages to adversaries at safe standoff ranges: 1) "You are detected"; and 2) "Lethal Weapons are likely aimed at you". Failure of an adversary to get the message can result in him being directly exposed to eye-safe glare or flashblinding to delay and disorient intruders. In the case of aggressors who choose to continue approaching controlled areas, a lethal response is an additional option.

Both Saber 203 and HALT programs have been conducted with the utmost diligence to assure resulting products are non-injurious to personnel, proven to minimize legal liabilities, and to comply with DoD Directive 3000.3 and other applicable guidance. Production is anticipated in the Fiscal Year 2001 time frame.

USAF SECURITY FORCES

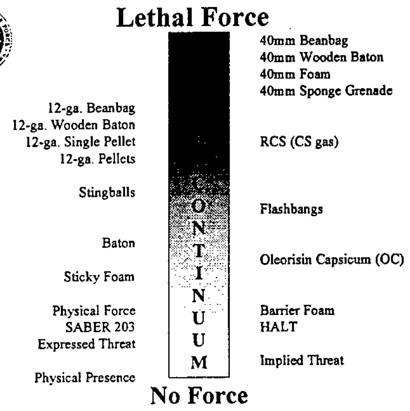
LASER ILLUMINATOR SYSTEMS

DEAN S. ADLER
Manager, Saber 203
Force Protection C2 SPO, ESC/FD
Hanscom AFB, MA
DSN 478-5997
COMM 617/377-5997
FAX 617/377-8832
E-Mail: adlerd@hanscom.af.mil

FOR OFFICIAL USE ONLY

POLICY FOR NON-LETHAL WEAPONS
DoD Directive 3000.3
July 1996

- Gives Commanders Flexibility In Employing Non-lethal Technologies And Allows Escalation To Deadly Force If Troops Are Threatened.
- States That Non-lethal Technologies Shall Not Be Required To Have A Zero Probability Of Producing Fatalities Or Permanent Injuries.
- Increases Options Available To A Commander To Minimize Fatalities, Permanent Injury And Undesired Damage To Property.
- Minimizes Need For Post Conflict Reconstruction, Allows Operations To Be Undertaken Where Lethal Force Is Not Viable And Limits The Escalation Of Violence In Peacekeeping Operations.
- Has As A Guideline That Non-lethal Effects Are Intended To Be Reversible.
- Shows Us Forces Are On A Humanitarian Mission And Do Not Want To Hurt Anyone.



Lethal Force

40mm Beanbag
40mm Wooden Baton
40mm Foam
40mm Sponge Grenade

12-ga. Beanbag
12-ga. Wooden Baton
12-ga. Single Pellet
12-ga. Pellets

RCS (CS gas)

Stingballs

Flashbangs

Baton

Oleorisin Capsicum (OC)

Sticky Foam

Physical Force
SABER 203
Expressed Threat

Barrier Foam
HALT

Implied Threat

Physical Presence

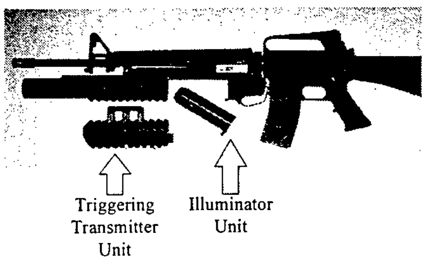
CONTINUUM

No Force

SYSTEM DESCRIPTION

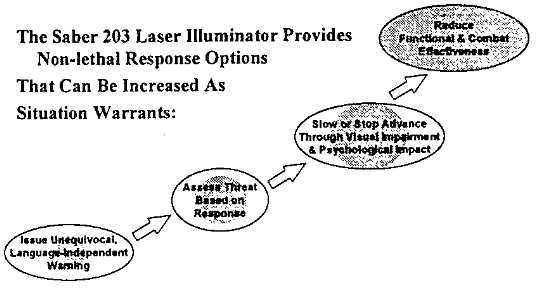
- Active CW Laser In Grenade Shell Form Factor To Operate On M-16/M-203 Weapon
- System Produces Glare In Eyes Of Intruder To Delay And Disorient At Close Range
- Illuminates Intruder At Long Ranges
- Intruder Choices: Retreat, Surrender, Or Signal Intent To Advance On Protected Asset
- User Can "Go Lethal" Quickly With M-16/M-203

LASER ILLUMINATOR ADDITIONS TO THE M203 WEAPON



SABER 203 CAPABILITIES

The Saber 203 Laser Illuminator Provides Non-lethal Response Options That Can Be Increased As Situation Warrants:

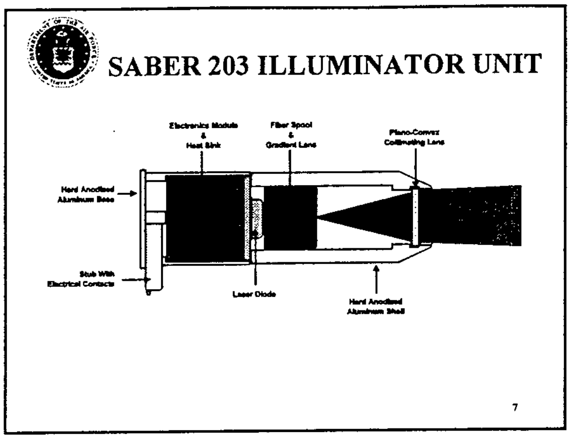


Issue Unequivocal, Language-Independent Warning

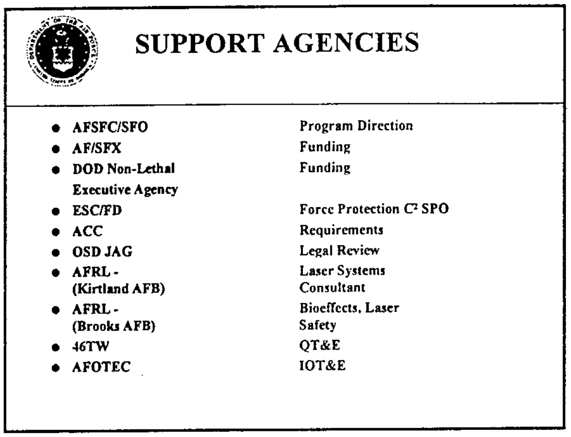
Assess Threat Based on Response

Slow or Stop Advance Through Visual Impairment & Psychological Impact

Reduce Functional & Combat Effectiveness

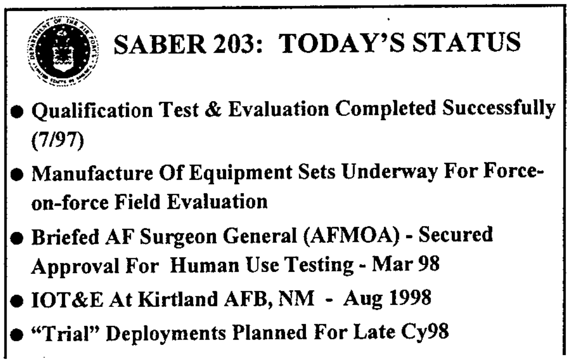


SABER 203 ILLUMINATOR UNIT



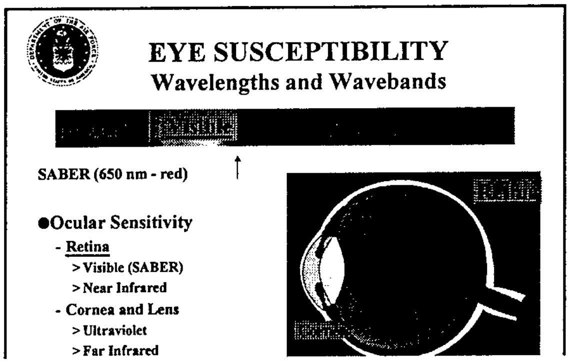
SUPPORT AGENCIES

• AFSFC/SFO	Program Direction
• AF/SFX	Funding
• DOD Non-Lethal Executive Agency	Funding
• ESC/FD	Force Protection C² SPO
• ACC	Requirements
• OSD JAG	Legal Review
• AFRL - (Kirtland AFB)	Laser Systems Consultant
• AFRL - (Brooks AFB)	Bioeffects, Laser Safety
• 46TW	QT&E
• AFOTEC	IOT&E



SABER 203: TODAY'S STATUS

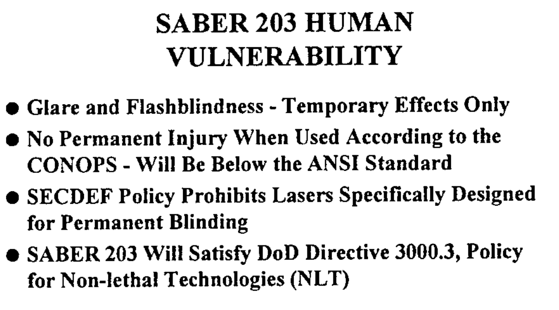
- Qualification Test & Evaluation Completed Successfully (7/97)
- Manufacture Of Equipment Sets Underway For Force-on-force Field Evaluation
- Briefed AF Surgeon General (AFMOA) - Secured Approval For Human Use Testing - Mar 98
- IOT&E At Kirtland AFB, NM - Aug 1998
- "Trial" Deployments Planned For Late Cy98



EYE SUSCEPTIBILITY
Wavelengths and Wavebands

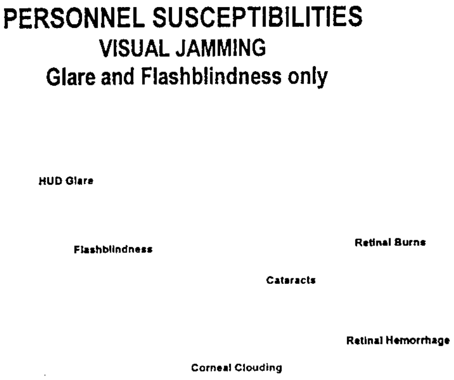
SABER (650 nm - red) ↑

- Ocular Sensitivity
  - Retina
    - > Visible (SABER)
    - > Near Infrared
  - Cornea and Lens
    - > Ultraviolet
    - > Far Infrared



SABER 203 HUMAN VULNERABILITY

- Glare and Flashblindness - Temporary Effects Only
- No Permanent Injury When Used According to the CONOPS - Will Be Below the ANSI Standard
- SECDEF Policy Prohibits Lasers Specifically Designed for Permanent Blinding
- SABER 203 Will Satisfy DoD Directive 3000.3, Policy for Non-lethal Technologies (NLT)



PERSONNEL SUSCEPTIBILITIES
VISUAL JAMMING
Glare and Flashblindness only

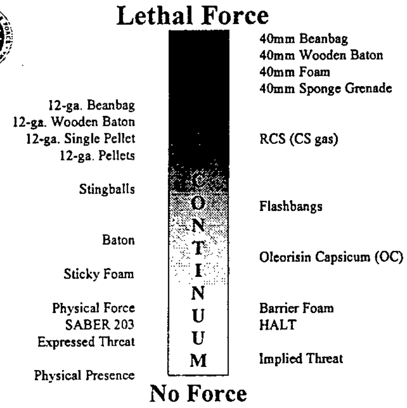
USAF SECURITY FORCES

LASER ILLUMINATOR SYSTEMS

DEAN S. ADLER
Manager, Saber 203
Force Protection C2 SPO, ESC/FD
Hanscom AFB, MA
DSN 478-5997
COMM 617/377-5997
FAX 617/377-8832
E-Mail: adlerd@hanscom.af.mil

POLICY FOR NON-LETHAL WEAPONS
DoD Directive 3000.3
July 1996

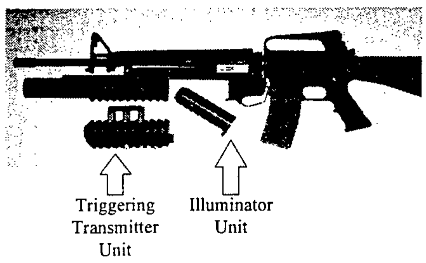
- Gives Commanders Flexibility In Employing Non-lethal Technologies And Allows Escalation To Deadly Force If Troops Are Threatened.
- States That Non-lethal Technologies Shall Not Be Required To Have A Zero Probability Of Producing Fatalities Or Permanent Injuries.
- Increases Options Available To A Commander To Minimize Fatalities, Permanent Injury And Undesired Damage To Property.
- Minimizes Need For Post Conflict Reconstruction, Allows Operations To Be Undertaken Where Lethal Force Is Not Viable And Limits The Escalation Of Violence In Peacekeeping Operations.
- Has As A Guideline That Non-lethal Effects Are Intended To Be Reversible.
- Shows Us Forces Are On A Humanitarian Mission And Do Not Want To Hurt Anyone.



SYSTEM DESCRIPTION

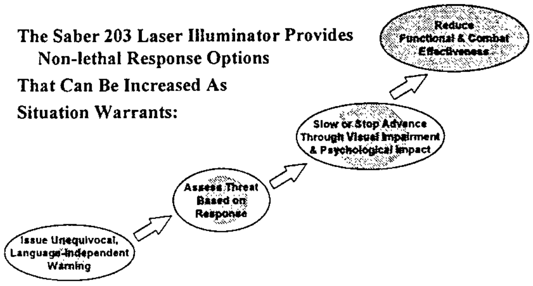
- Active CW Laser In Grenade Shell Form Factor To Operate On M-16/M-203 Weapon
- System Produces Glare In Eyes Of Intruder To Delay And Disorient At Close Range
- Illuminates Intruder At Long Ranges
- Intruder Choices: Retreat, Surrender, Or Signal Intent To Advance On Protected Asset
- User Can "Go Lethal" Quickly With M-16/M-203

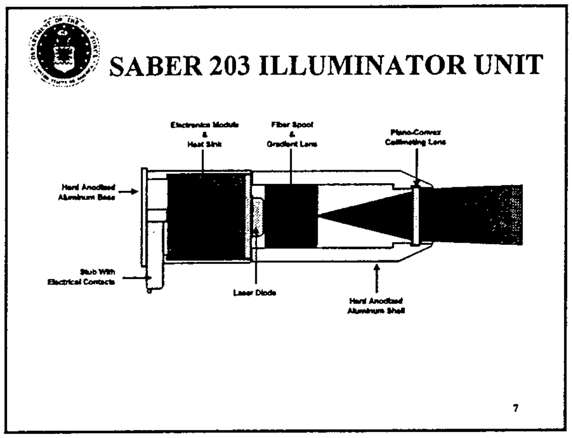
LASER ILLUMINATOR ADDITIONS TO THE M203 WEAPON



SABER 203 CAPABILITIES

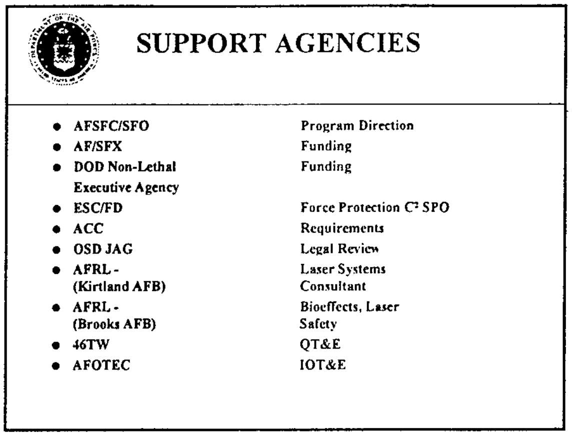
The Saber 203 Laser Illuminator Provides Non-lethal Response Options That Can Be Increased As Situation Warrants:


Issue Unequivocal, Language-Independent Warning
Assess Threat Based on Response
Slow or Stop Advance Through Visual Impairment & Psychological Impact
Reduce Functional & Combat Effectiveness



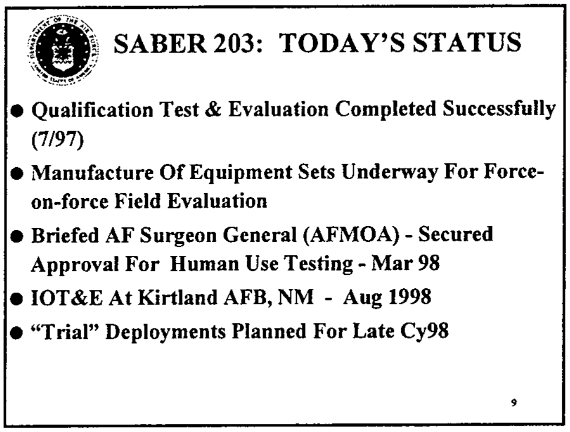
SABER 203 ILLUMINATOR UNIT

Electronics Module & Heat Sink
Fiber Spool & Gradient Lens
Plano-Convex Collimating Lens
Hard Anodized Aluminum Base
Stub With Electrical Contacts
Laser Diode
Hard Anodized Aluminum Shell



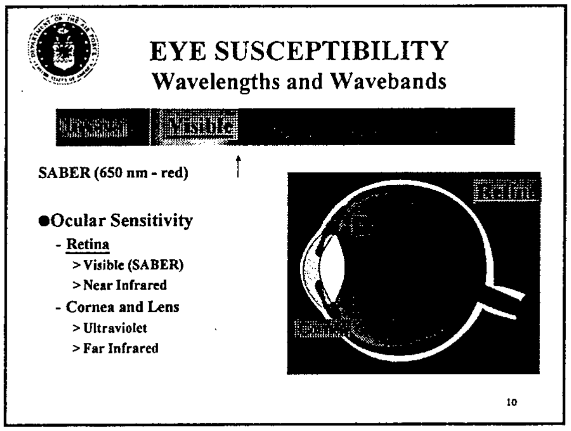
SUPPORT AGENCIES

● AFSFC/SFO	Program Direction
● AF/SFX	Funding
● DOD Non-Lethal Executive Agency	Funding
● ESC/FD	Force Protection C² SPO
● ACC	Requirements
● OSD JAG	Legal Review
● AFRL - (Kirtland AFB)	Laser Systems Consultant
● AFRL - (Brooks AFB)	Bioeffects, Laser Safety
● 46TW	QT&E
● AFOTEC	IOT&E



SABER 203: TODAY'S STATUS

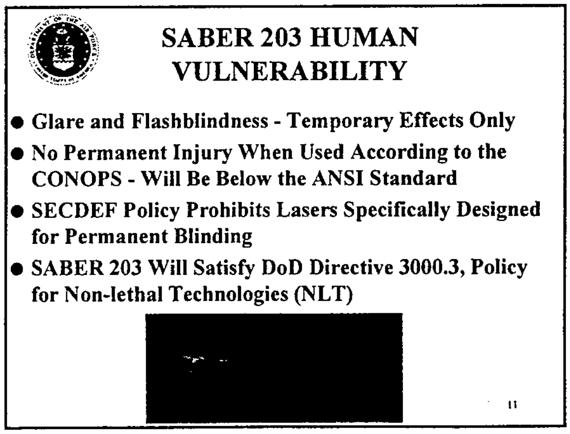
- Qualification Test & Evaluation Completed Successfully (7/97)
- Manufacture Of Equipment Sets Underway For Force-on-force Field Evaluation
- Briefed AF Surgeon General (AFMOA) - Secured Approval For Human Use Testing - Mar 98
- IOT&E At Kirtland AFB, NM - Aug 1998
- "Trial" Deployments Planned For Late Cy98



EYE SUSCEPTIBILITY
Wavelengths and Wavebands

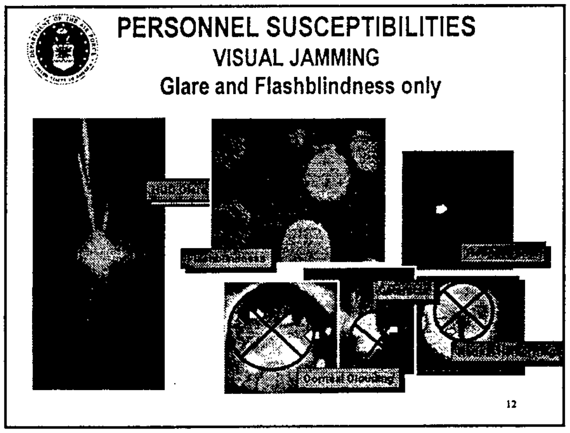
SABER (650 nm - red)

- Ocular Sensitivity
  - Retina
    - > Visible (SABER)
    - > Near Infrared
  - Cornea and Lens
    - > Ultraviolet
    - > Far Infrared



SABER 203 HUMAN VULNERABILITY

- Glare and Flashblindness - Temporary Effects Only
- No Permanent Injury When Used According to the CONOPS - Will Be Below the ANSI Standard
- SECDEF Policy Prohibits Lasers Specifically Designed for Permanent Blinding
- SABER 203 Will Satisfy DoD Directive 3000.3, Policy for Non-lethal Technologies (NLT)



PERSONNEL SUSCEPTIBILITIES
VISUAL JAMMING
Glare and Flashblindness only

SABER 203 EYE SAFETY CONCLUSIONS

- AFRL/HEDO Will Assure Eye Safety Prior to QOT&E
  - Effective Dosage Studies
  - SABER Laser Beam Characterizations
  - A Thorough Human Use Review Process
  - Subject Safety Briefings, System Training, and Eye Exams
- The SABER 203 Laser Illuminator Will Be Eye-safe If Used Within the Guidance of the CONOPS
- There Will Be No Eye Injuries for Laser Exposures That Are Within the ANSI Standards ... Including SABER 203!

HALT

HINDERING ADVERSARIES WITH LESS-THAN-LETHAL TECHNOLOGY (HALT)

A USAF "Spiral" Development Program Derived from Saber 203

DEAN S. ADLER
Manager, Saber 203
ESC/FD
Force Protection C^2 SPO
Hanscom AFB, MA

SABER & HALT COMPARISON

HALT

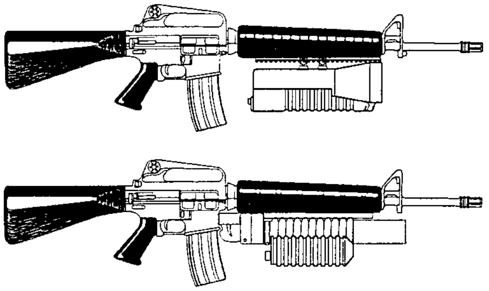
- HALT Will Be Eye Safe At The Aperture; Saber Has A Nominal Ocular Hazard Distance Of 6 Meters
- HALT Will Mount To Any Weapon (M-16 Initially); Saber Limited To M-203
- HALT Will Be Capable Of Autonomous, Hand-held Operation (EMD Configuration)
- HALT Can Provide Area Illumination To Ranges In Excess Of 800m - Allows Engaging Threats At The Max. Range Of The M-16 Rifle

FOR THESE REASONS,
HALT IS VIEWED AS BEING OF SIGNIFICANT PRODUCTION POTENTIAL FOR THE MULTI-SERVICES

HALT SYSTEM (as of January PMR)

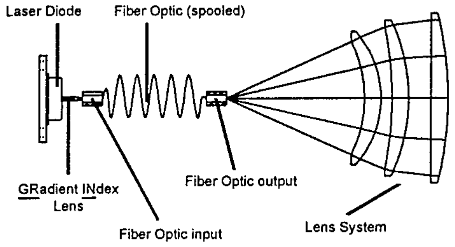
COMPARISON TO SABER 203 SYSTEM

HALT



OPTICAL SYSTEM GENERAL LAYOUT

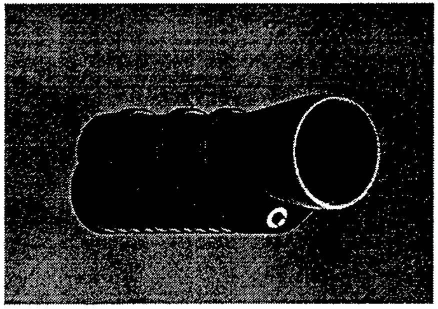
HALT

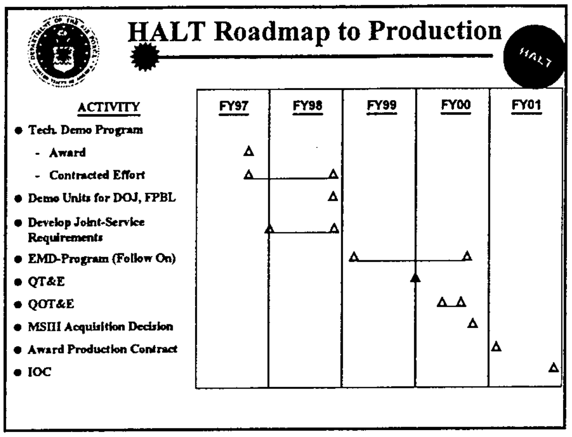


HALT Mechanical Design

Solid Model of Device

HALT

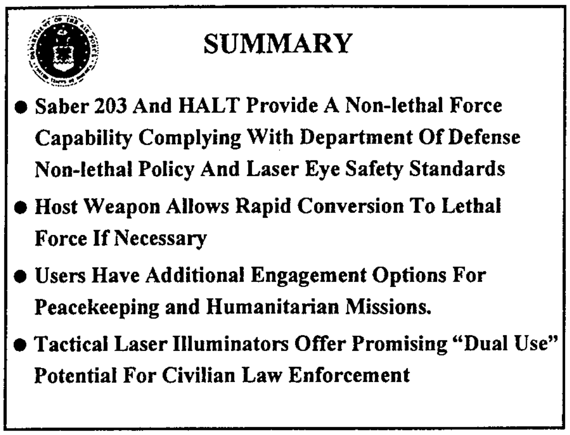




HALT Roadmap to Production

ACTIVITY

- Tech. Demo Program
  - Award
  - Contracted Effort
- Demo Units for DOJ, FPBL
- Develop Joint-Service Requirements
- EMD-Program (Follow On)
- QT&E
- QOT&E
- MSIII Acquisition Decision
- Award Production Contract
- IOC



SUMMARY

- Saber 203 And HALT Provide A Non-lethal Force Capability Complying With Department Of Defense Non-lethal Policy And Laser Eye Safety Standards
- Host Weapon Allows Rapid Conversion To Lethal Force If Necessary
- Users Have Additional Engagement Options For Peacekeeping and Humanitarian Missions.
- Tactical Laser Illuminators Offer Promising "Dual Use" Potential For Civilian Law Enforcement

IDS Intelligent Detection Systems Inc.

Specialists in Chemical Detection

Detection of Explosives, Narcotics and Chemical Warfare Agents by Fast GC-IMS Based Systems

By
Dr. Lawrence V.Haley
Vice President, Research and Development
and
Julian M. Romeskie, P. Eng.
Vice President, Marketing & Business Development

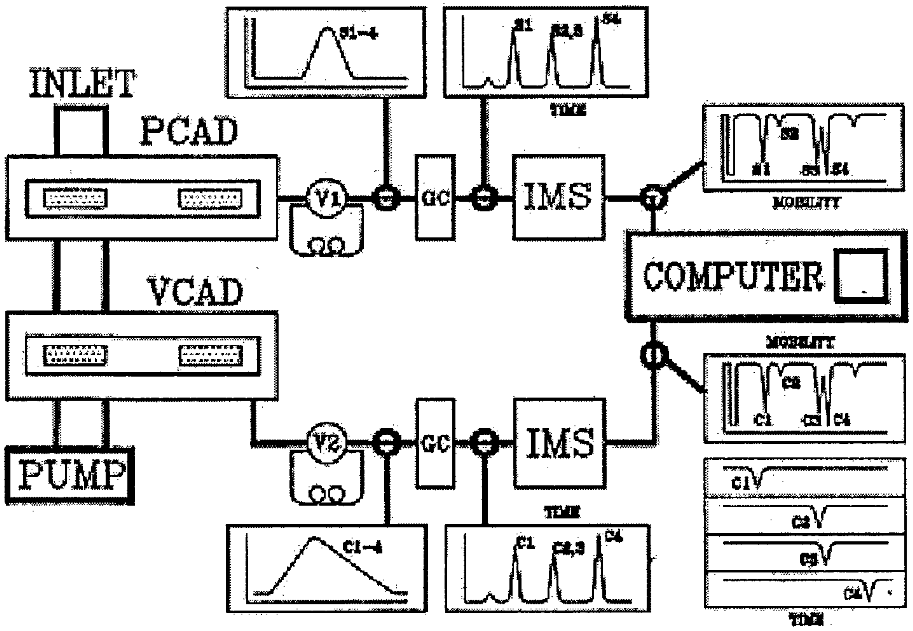
Corporate Background

- Founded in 1986 as CPAD Holdings Inc.
- Specialists in chemical detection technology
  - focused on explosives & drug trace detection
  - technology patented worldwide
- Operations in US, Canada, the United Kingdom and Europe
- Worldwide distribution and support
- IDS is publicly traded on the TSE

IDS products use patented GC/IMS technologies

The only GC/IMS based product with simultaneous detection of:

- particles and vapors
- explosives and drugs



Benefits

- high detection rate
  - sensitivity and selectivity
- low false alarm rate
- high throughput rate
- low maintenance

Explosives Detection

Counter Terrorism Focused

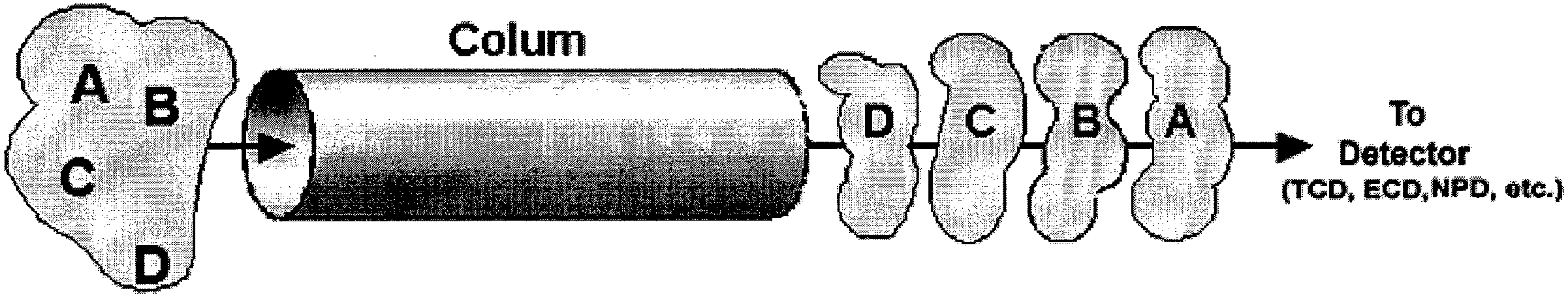
- Aviation - checked and carry-on baggage
  - driven by Air India and Pan Am disasters
- Building protection
  - driven by World Trade Center, Oklahoma City bombings
- Military installations
  - driven by Lebanon and Khobar bombings

Drug Detection

Drug Interdiction

- Border Control Points
- Correctional Facilities
- Seaports
- Transportation

Gas Chromatography

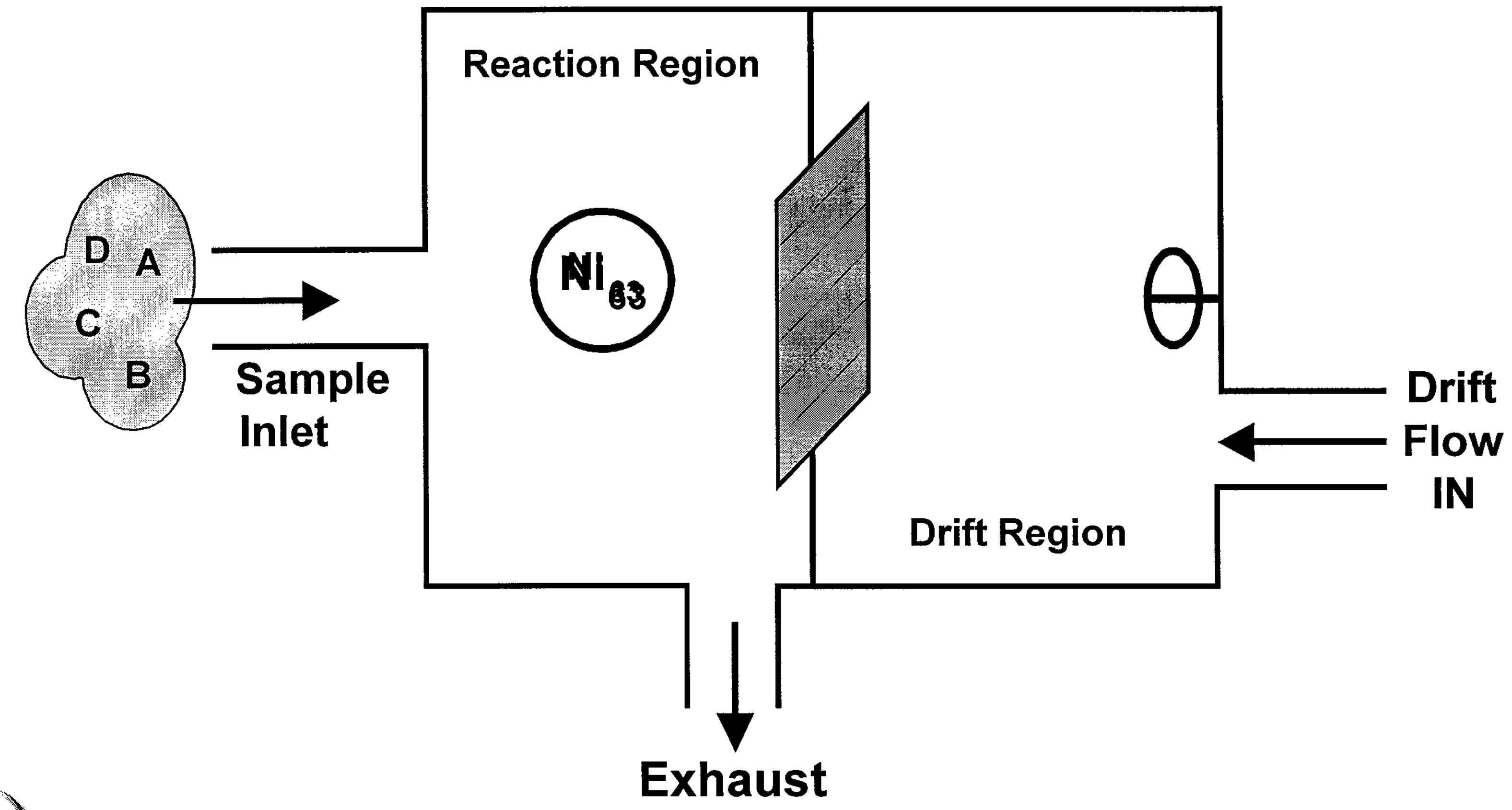


Sample
Mixture
In

- A -Fastest
- B -Fast
- C - Slow
- D - Slowest

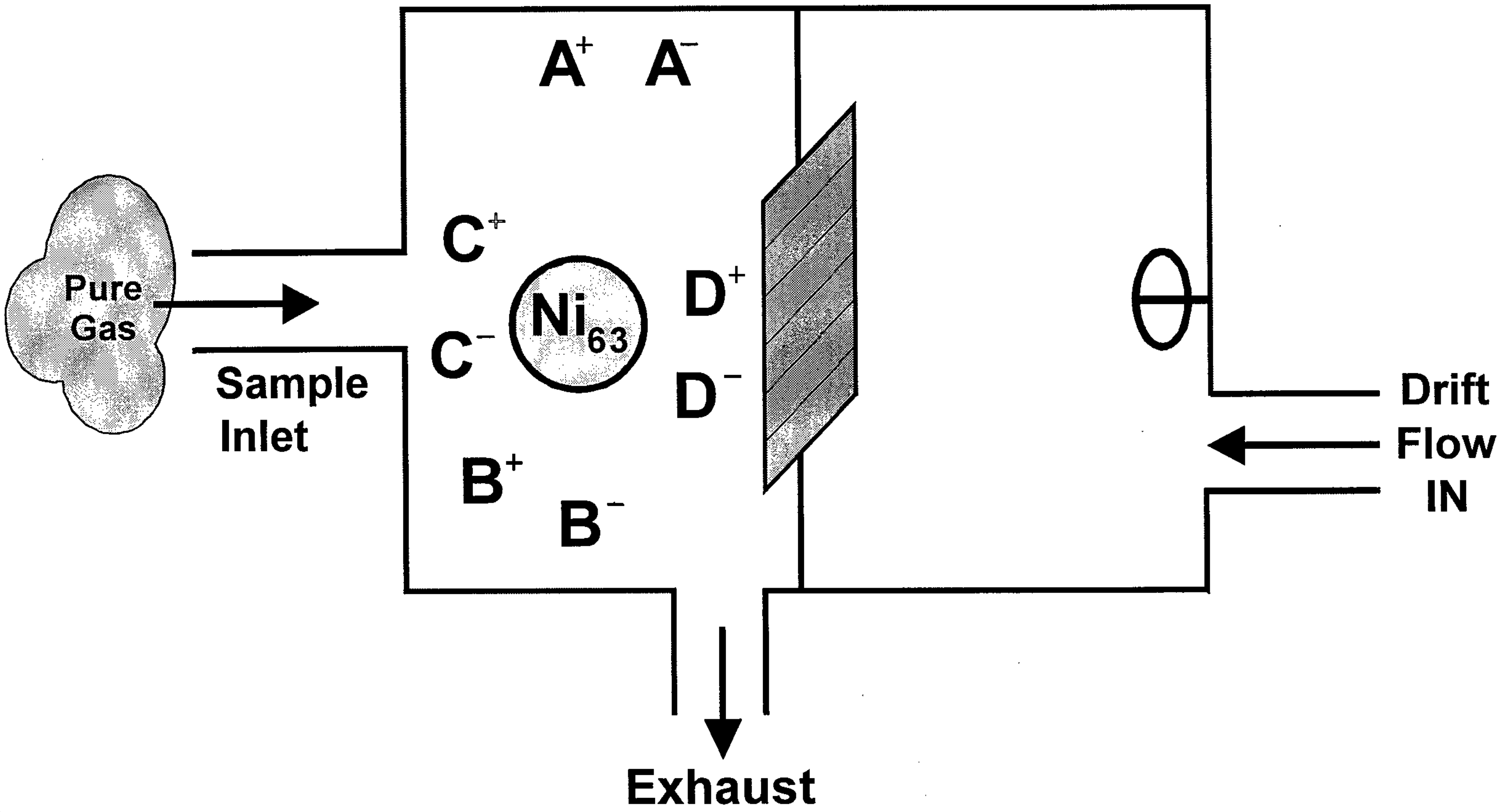
IMS - Analytical Process Description

Step 1 - Sample Injection



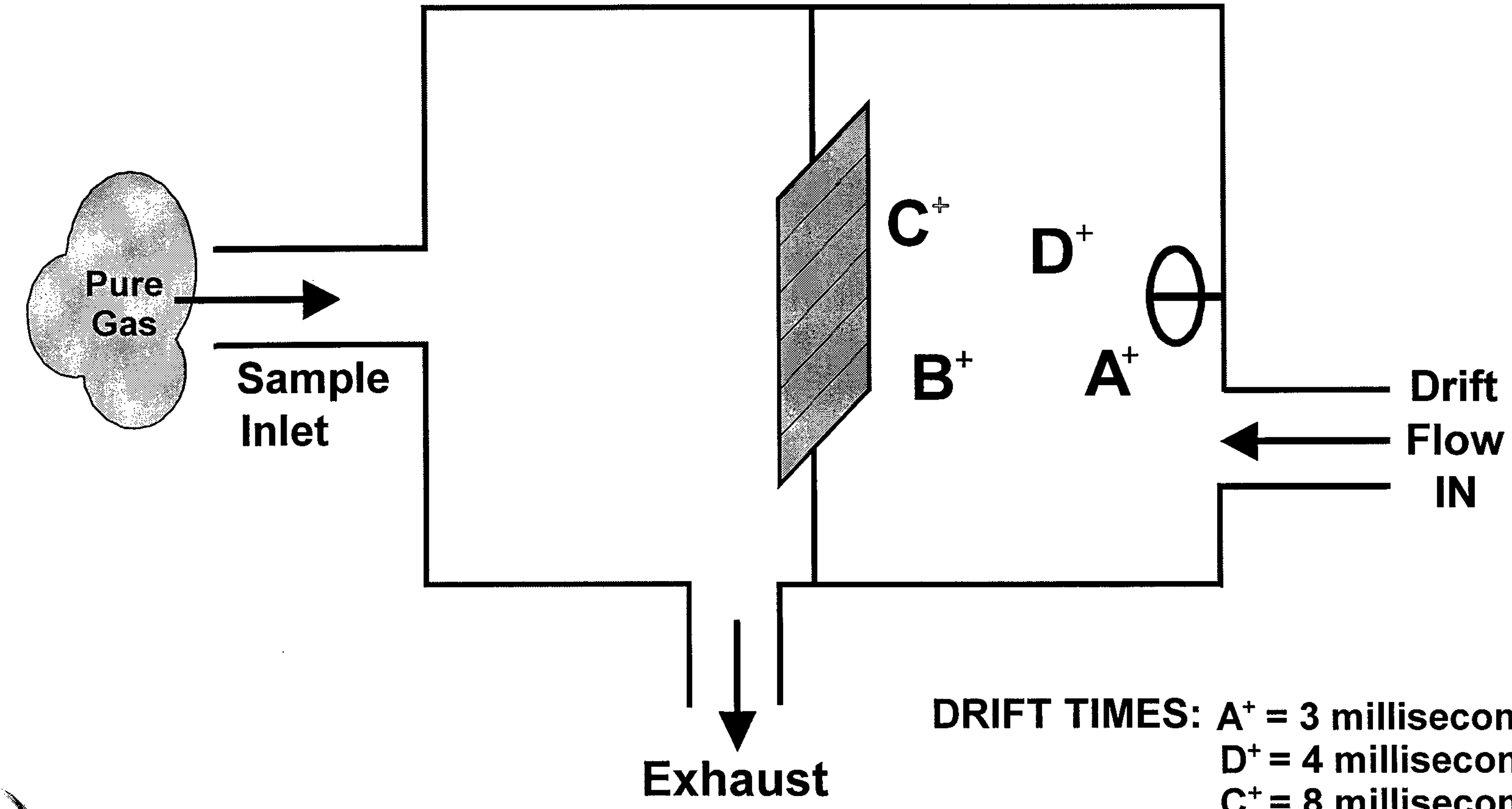
IMS - Analytical Process Description

Step 2 - Ionization



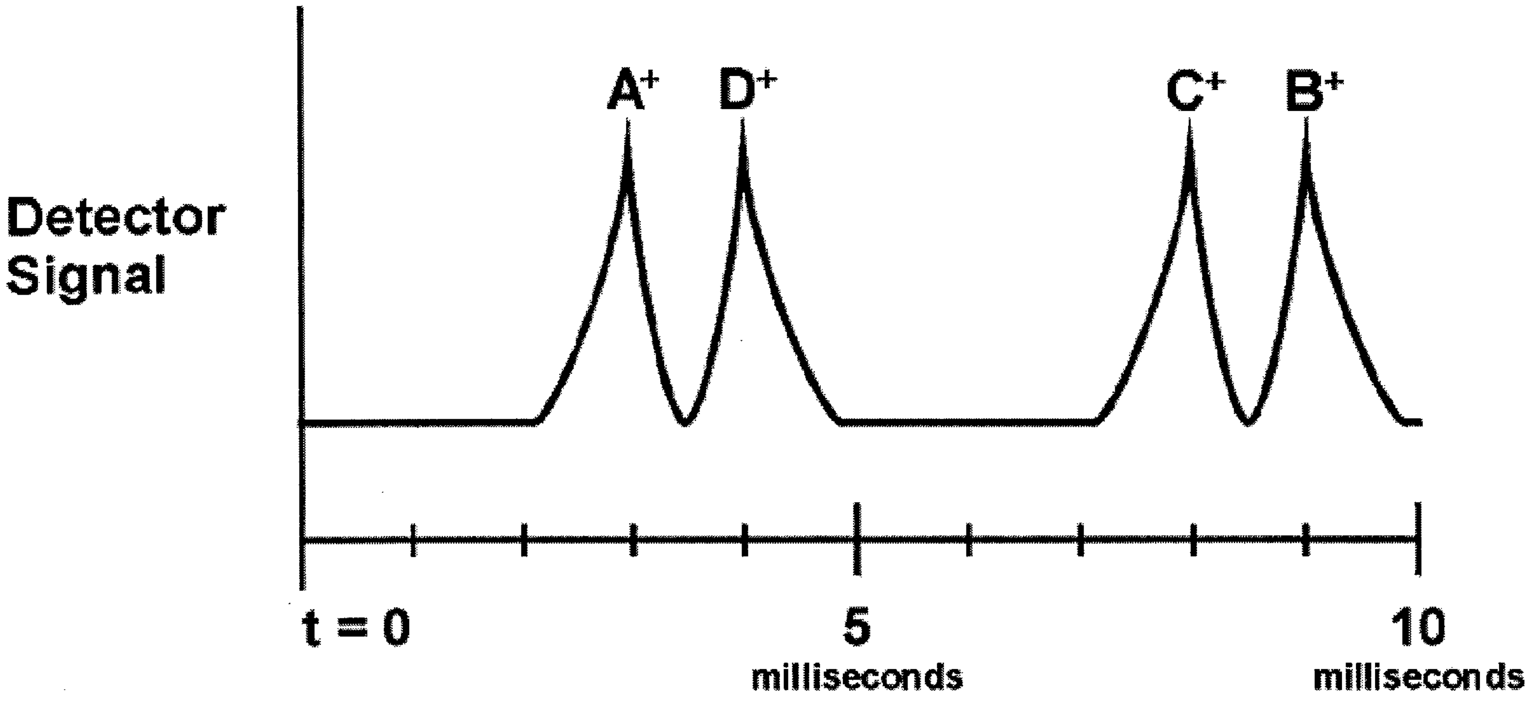
IMS - Analytical Process Description

Step 3 - Ion Separation and Detection



DRIFT TIMES: A^+ = 3 milliseconds
D^+ = 4 milliseconds
C^+ = 8 milliseconds
B^+ = 9 milliseconds

Graphical Representation of the IMS Output Signal



Note: This is ONE waveform

Basic Equations

GC:

$N=5.54(t_R/w_b)$ Plate Number

t_R= Retention Time
w_b= half height width

$H=L/N$ Plate Height (also, HETP)

L= length of column

$R_S=d/w_b$ Resolution

d= Distance between two peaks

Stationary Phase Polarity

IMS:

$V_d= K \times E$ Drift Velocity

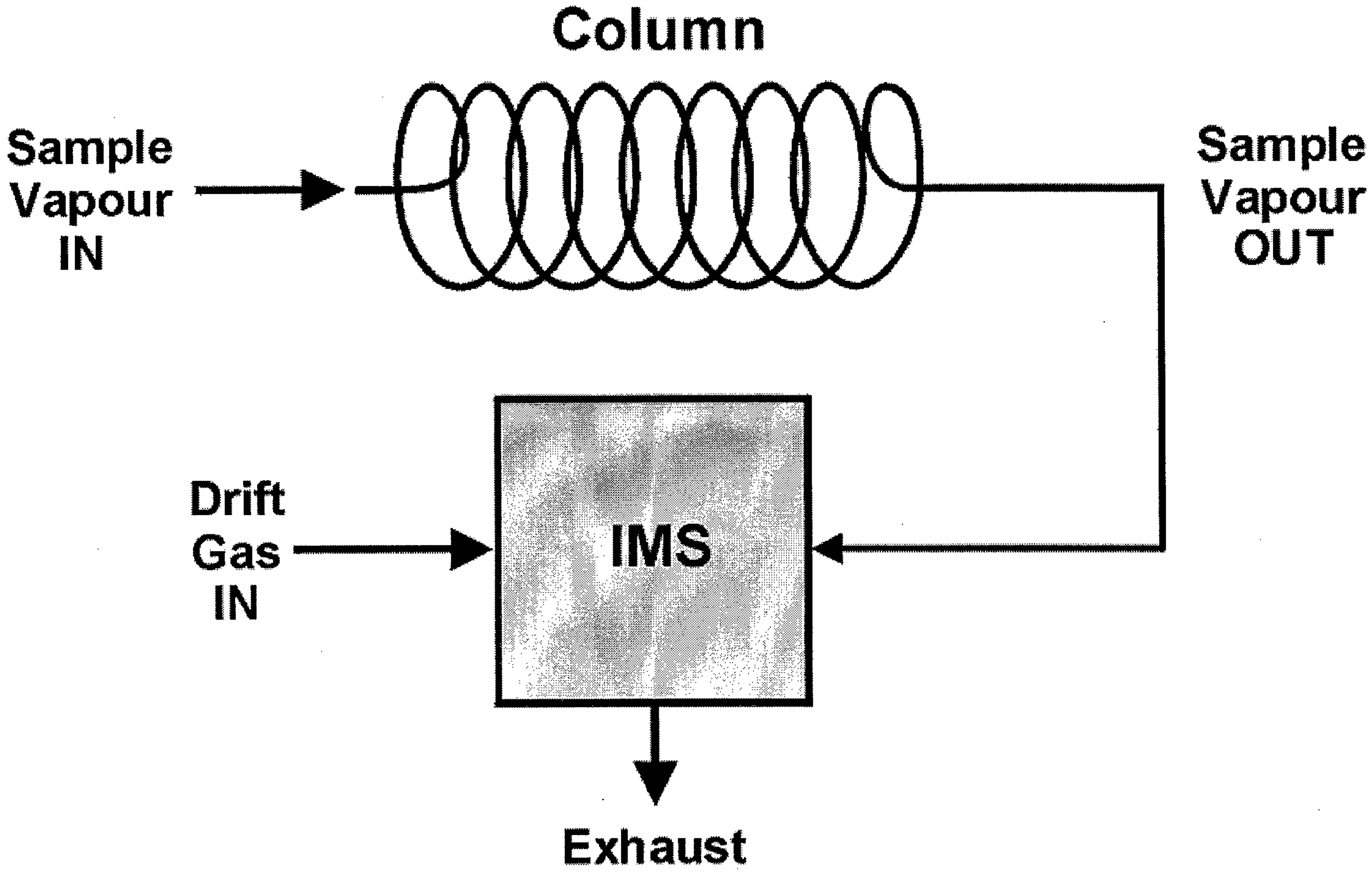
E= Drift Field Strength
K= Ion Mobility

$K= d/(t_dE)$ or $d^2/(t_dV_e)$ Mobility

t_d = Drift Time
d = Drift Region Length
V_e= Voltage

$K_0= K(P/760)(273/T)$ Reduced Mobility

GC - IMS Technology



Column

Sample
Vapour
IN

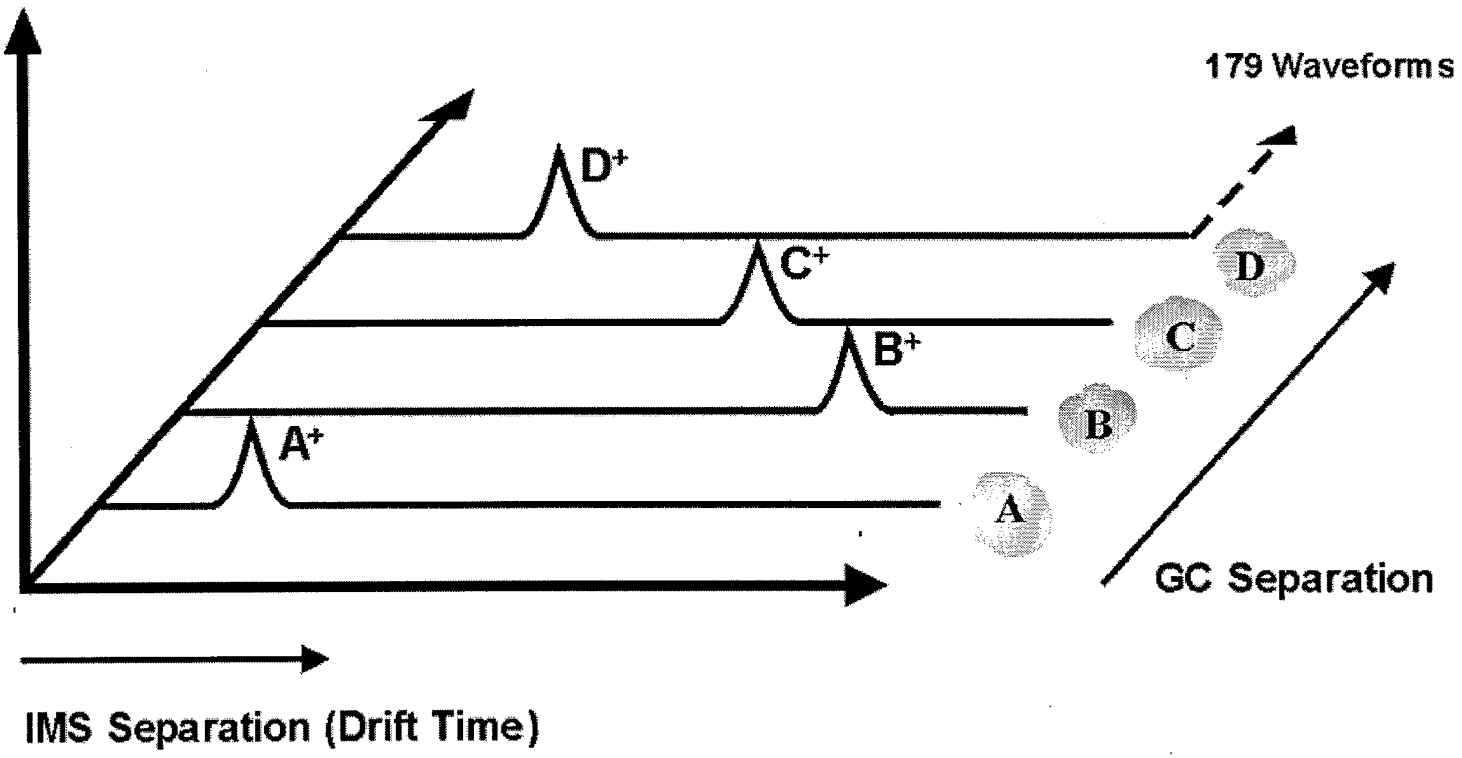
Sample
Vapour
OUT

Drift
Gas
IN

IMS

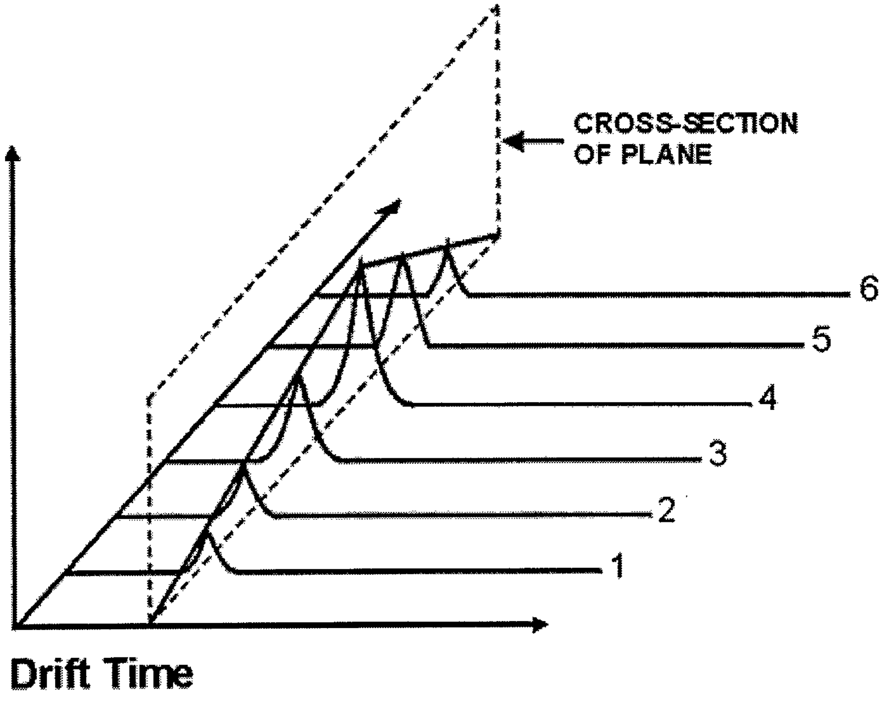
Exhaust

Graphical Representation of the GC-IMS Output Signal

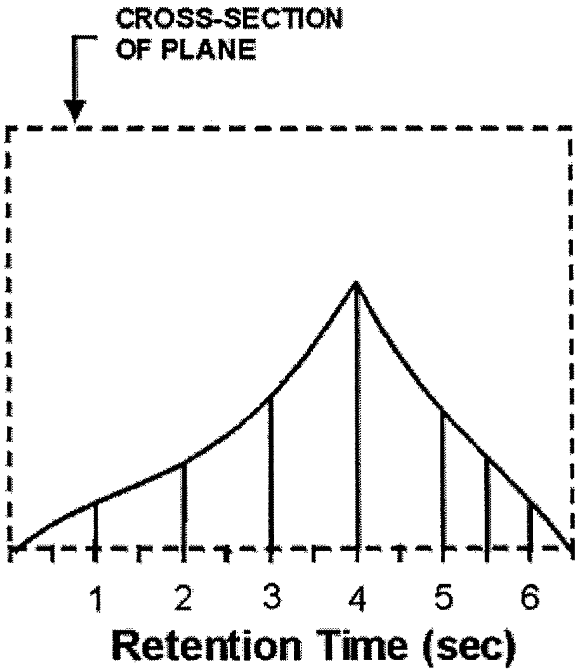


GC Projection of a Single Ion Peak

Continuity of Peaks

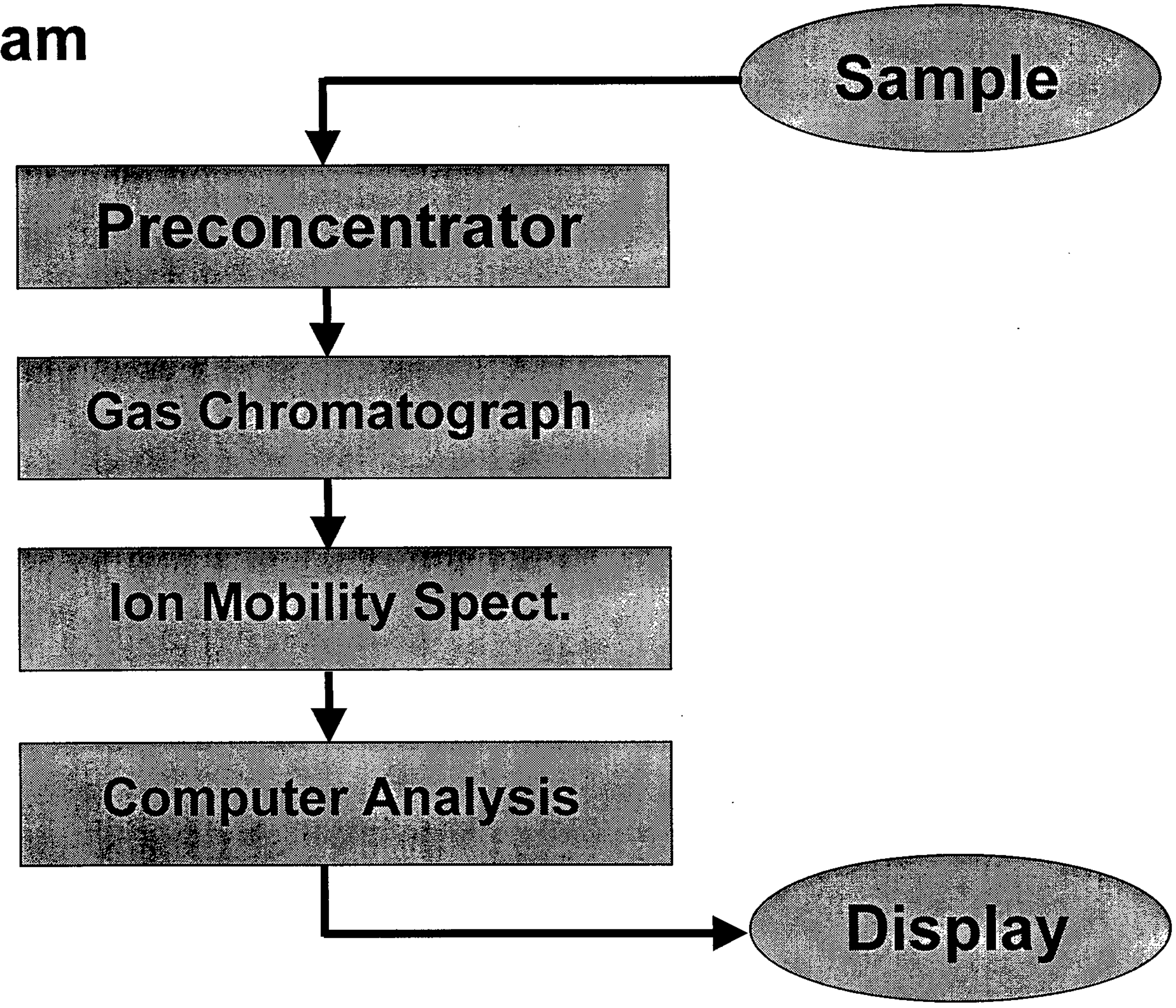


GC Signal That is Calculated Right Now



Trace-Compound Detection System

Block Diagram



Sample

Preconcentrator

Gas Chromatograph

Ion Mobility Spect.

Computer Analysis

Display

IDS Products

Orion & Orion Plus

- a console-type detection system for explosives and ICAO taggants

Ariel

- a console-type detection system for drugs

Sirius

- a console-type detection system for explosives and drugs

Walk-through

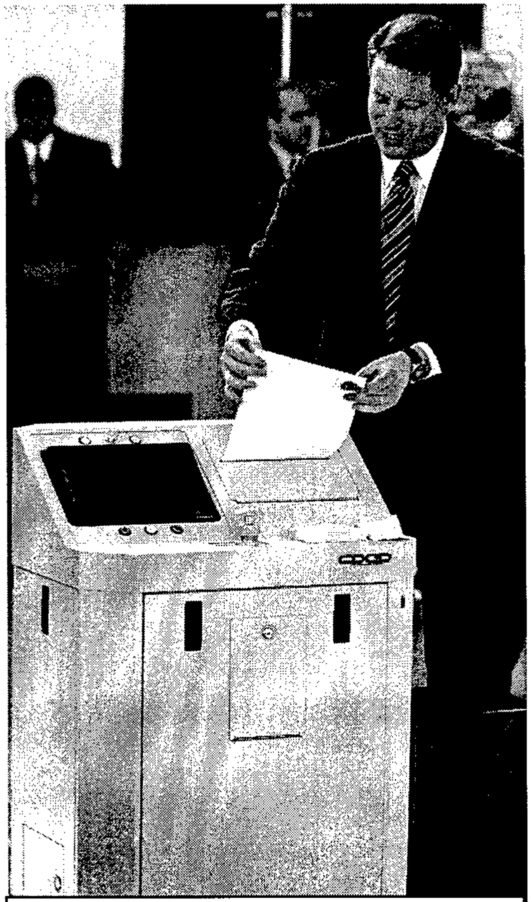
- a portal-type explosives detection system (EDS) for passenger walk-through

V-bEDS

- a portal-type EDS for vehicles

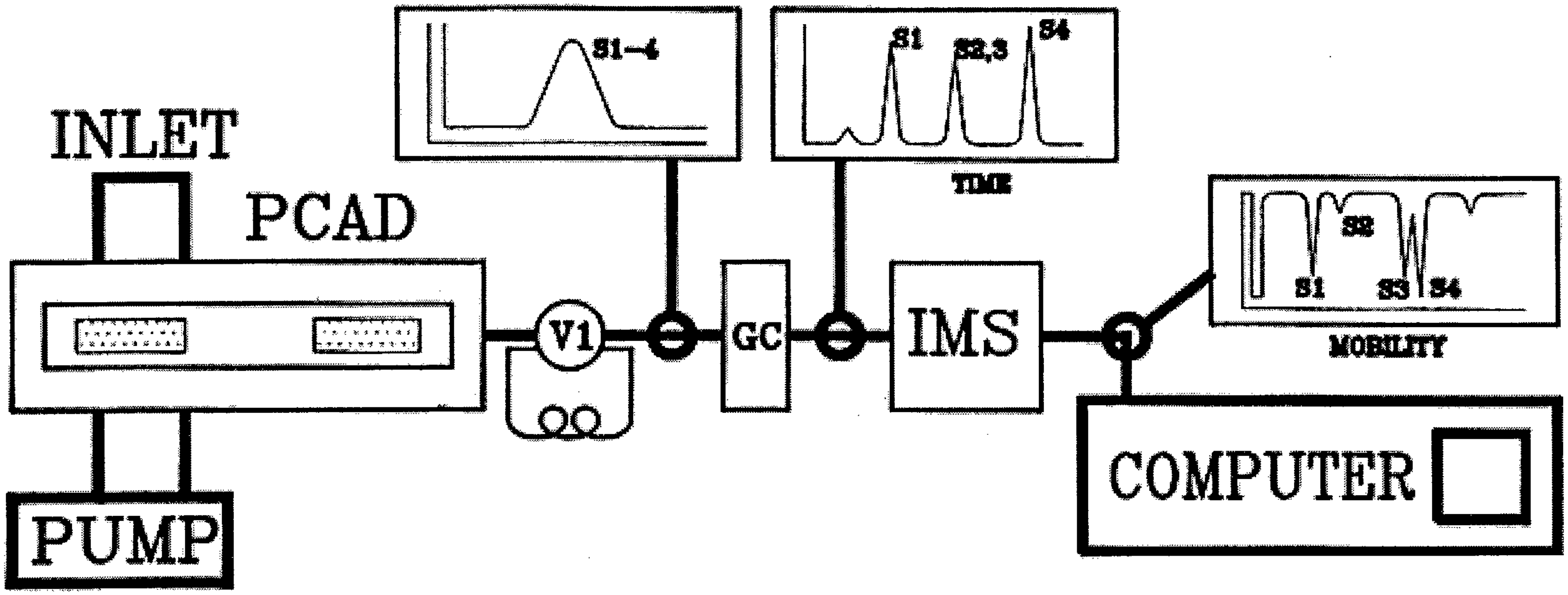
Orion & Orion$^+$

- Dual technology GC/IMS
- Self-contained and easy to use
  - built-in PC and touch screen display
- Fast one-step sampling process
  - ensures high throughput rate
- Detects ICAO taggants (Orion$^+$)
- Low maintenance
  - low cost consumables
- Remote sampling capability

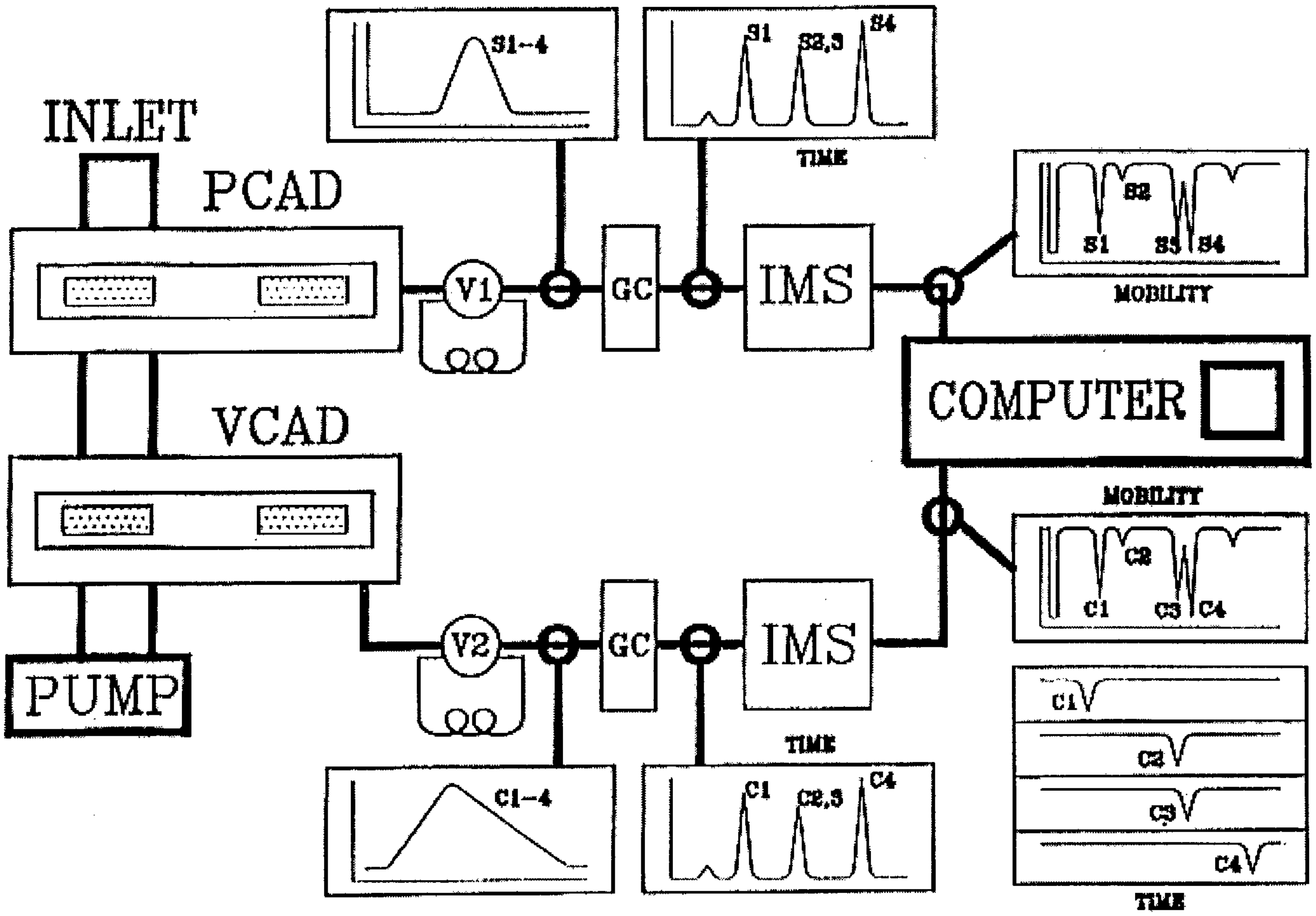


Vice President Al Gore examines an IDS Orion+ at San Francisco International Airport

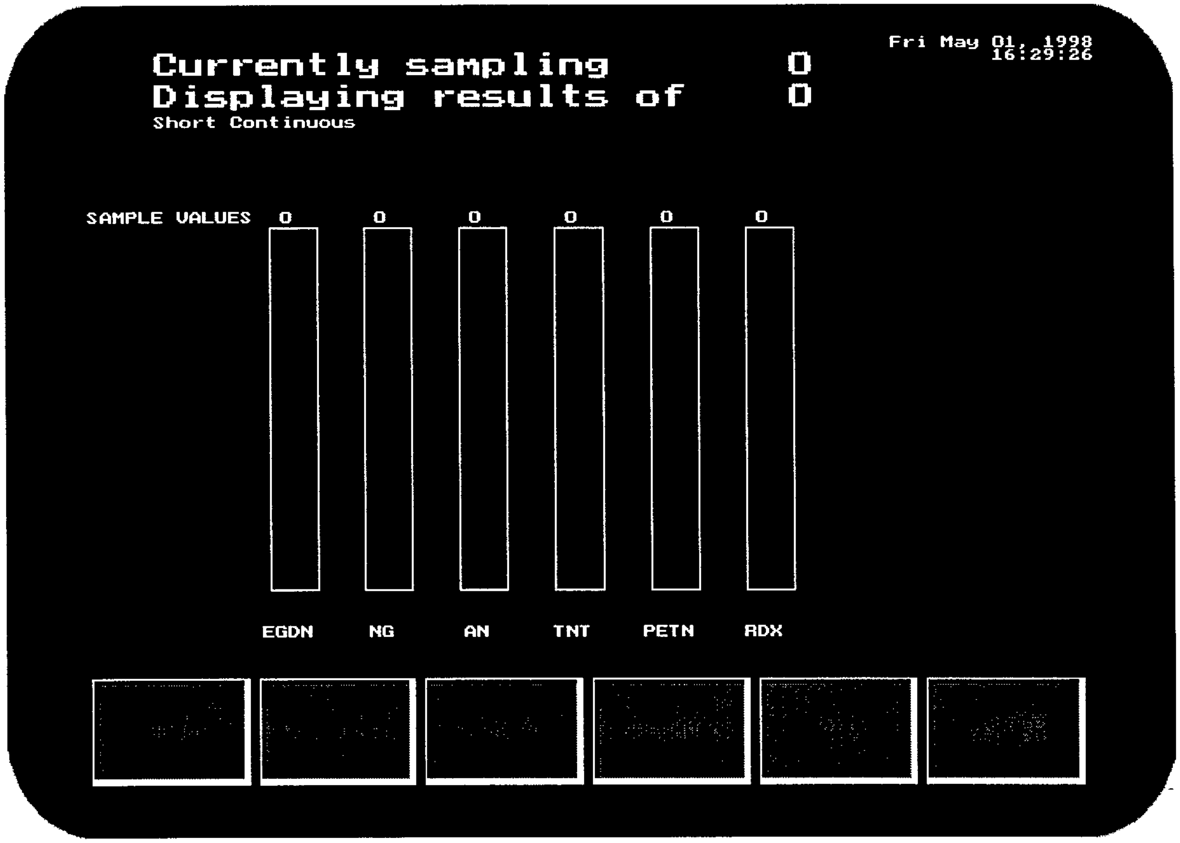
Orion Explosive Detection System Schematic



Orion Plus Detection System Schematic



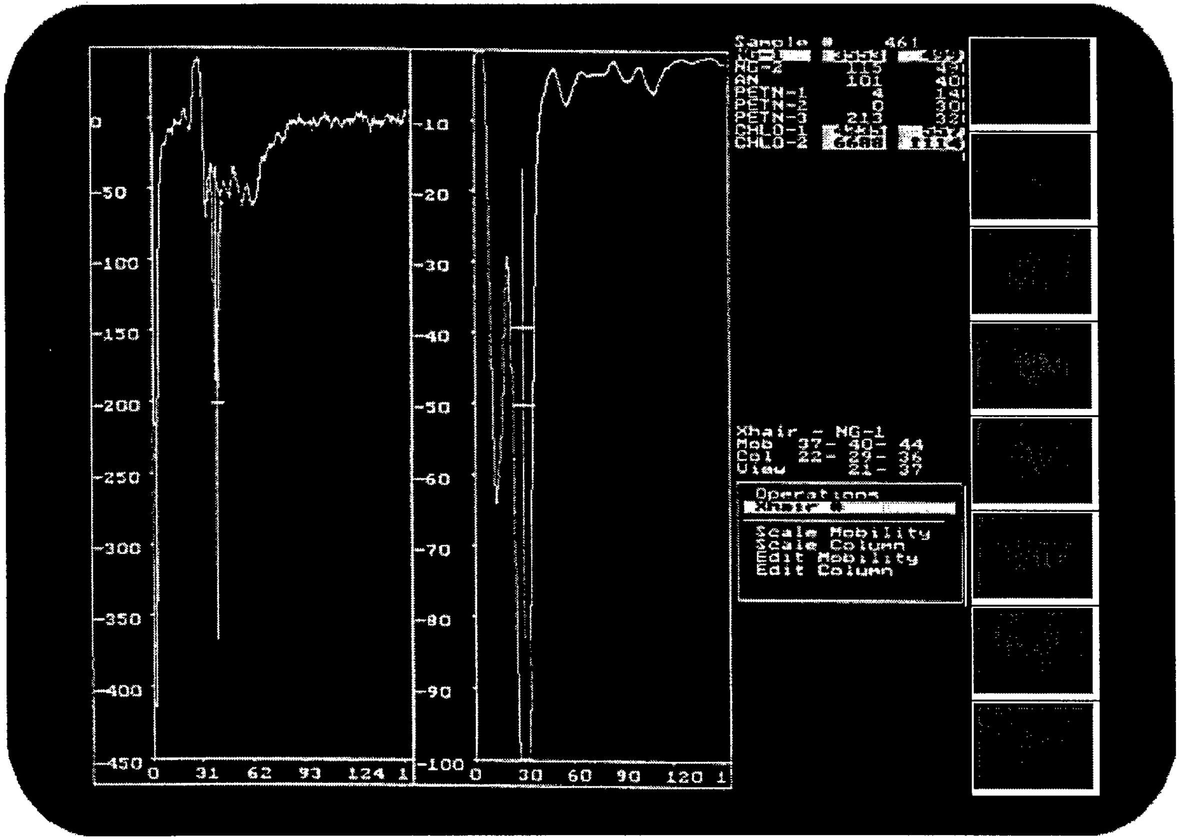
Barscreen Display of the Orion+



Fri May 01, 1998
16:29:26

Currently sampling 0
Displaying results of 0
Short Continuous

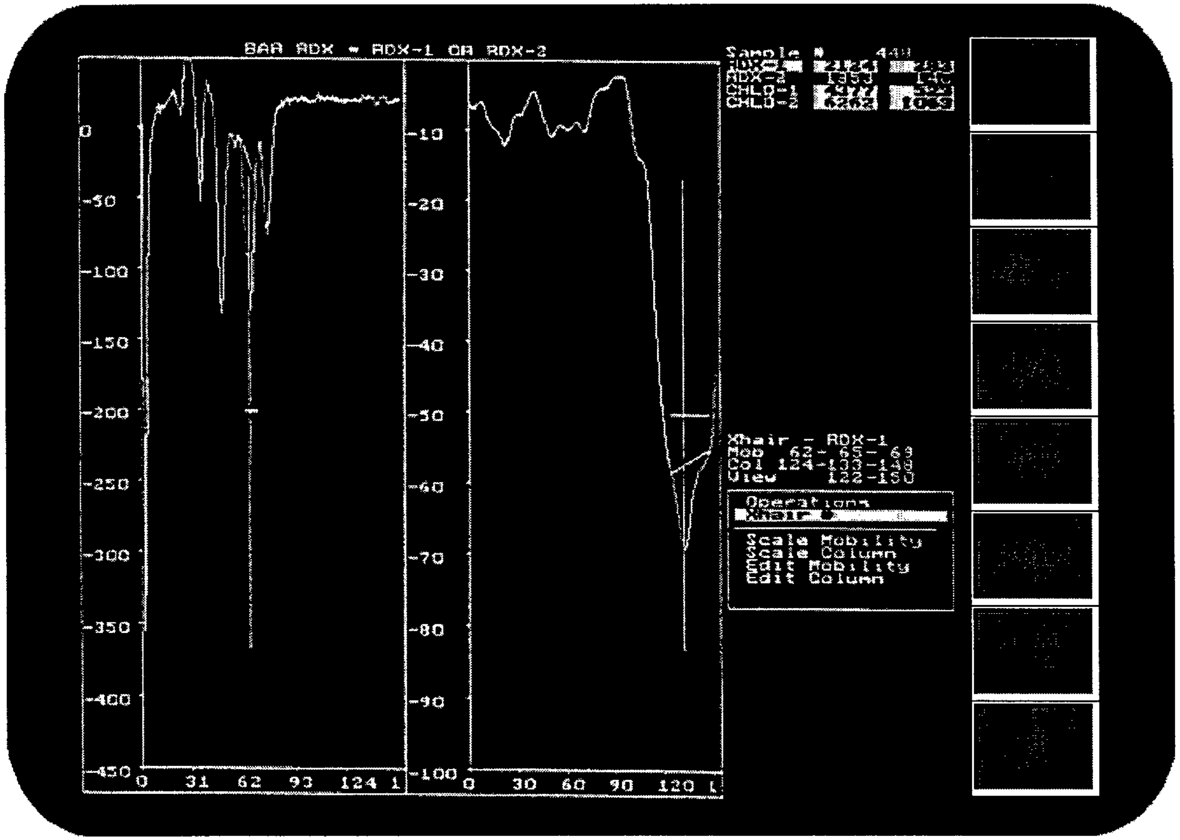
Analog Display Readout of NG



```
Sample #      461
[illegible]   [illegible]  [illegible]
NG-2          115          4[illegible]
AN            101          40
PETN-1          4          14
PETN-2          0          30
PETN-3        213          32
CHLO-1        [illegible]  [illegible]
CHLO-2        6688         [illegible]

Xhair - NG-1
Mob  37- 40- 44
Col  22- 29- 36
View     21- 37
```

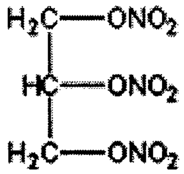
Analog Display Readout of RDX



```
Sample #    448
RDX-1   [illegible]  [illegible]
RDX-2    1353     140
CHLO-1  [illegible]  [illegible]
CHLO-2   6262    10.9
```

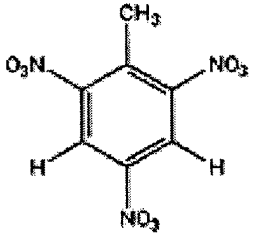
```
Xhair - RDX-1
Mob  62- 65- 68
Col 124-133-148
View    122-150
```

Molecular Structure and Vapour Pressure



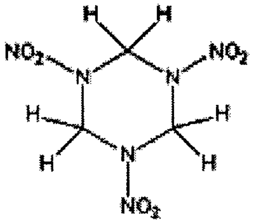
NG

MW-227
VP-459 PPB



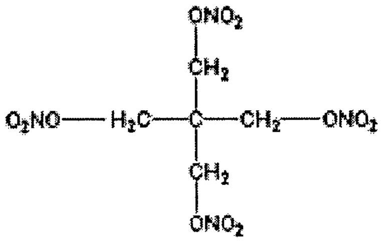
TNT

MW-227
VP-8 PPB



RDX

MW-222
VP-0.0056 PPB

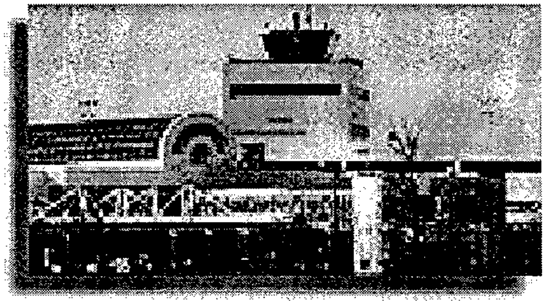


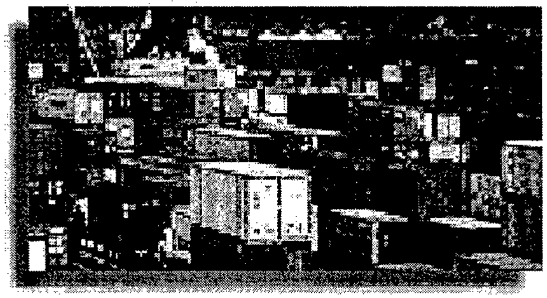
PETN

MW-316
VP-0.018 PPB

Ariel and Sirius

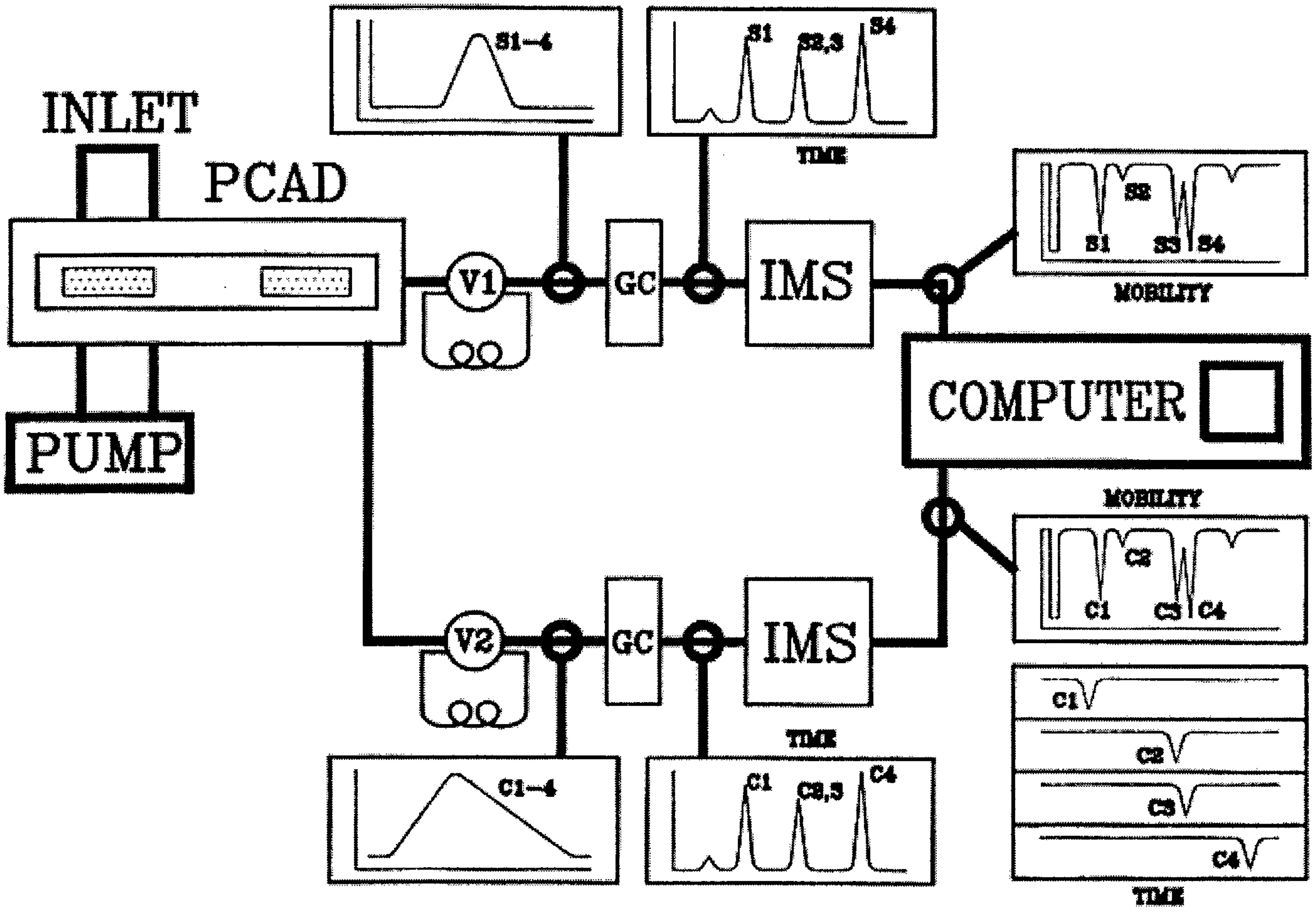
- **Ariel** - illicit drug detection
- **Sirius** - explosives and drug detection



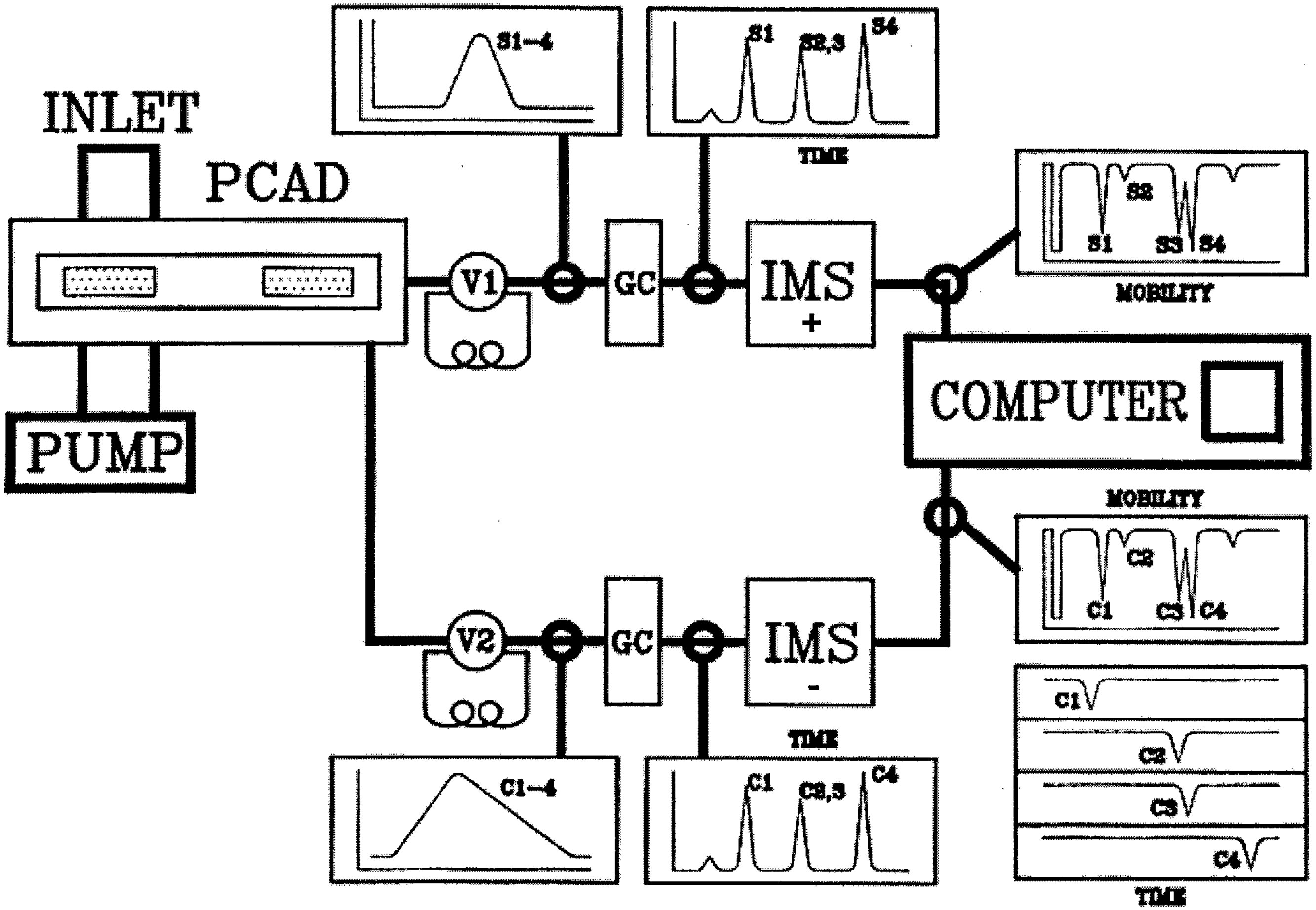


- **Common characteristics:**
  - GC/IMS dual technology
  - fast one-step process
  - self contained unit
  - remote sampling unit (RSU)
  - built-in PC and display

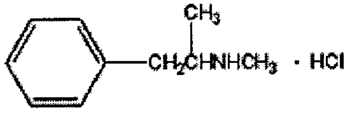
Ariel Narcotics Detection System Schematic



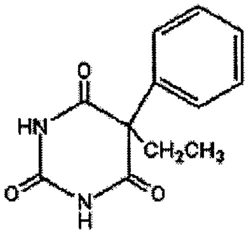
Sirius Explosive/Drug Detection System Schematic



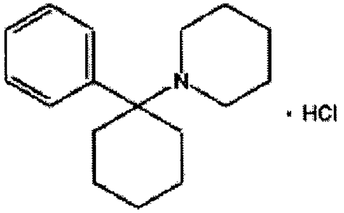
Typical Target Drug Compounds



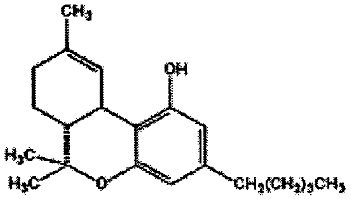
METHAMPHETAMINE



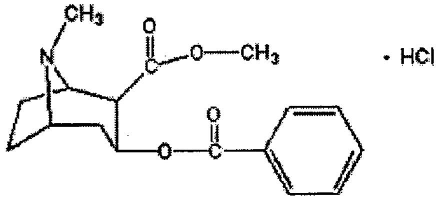
PHENOBARBITAL



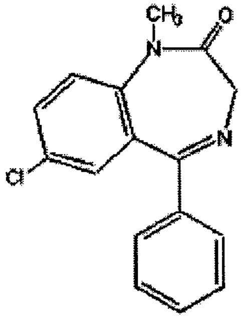
PCP



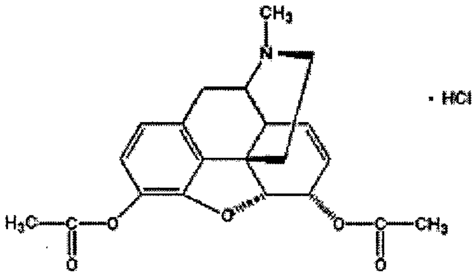
THC



COCAINE



DIAZEPAM



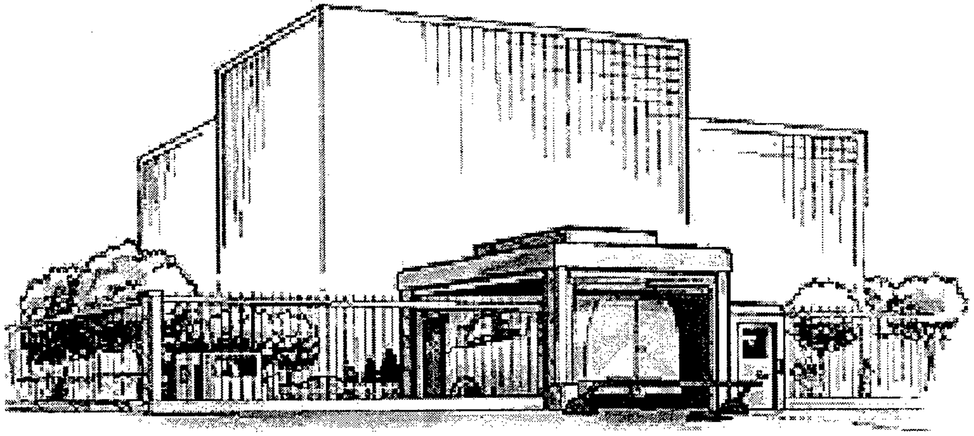
HEROIN

Walk-Through EDS

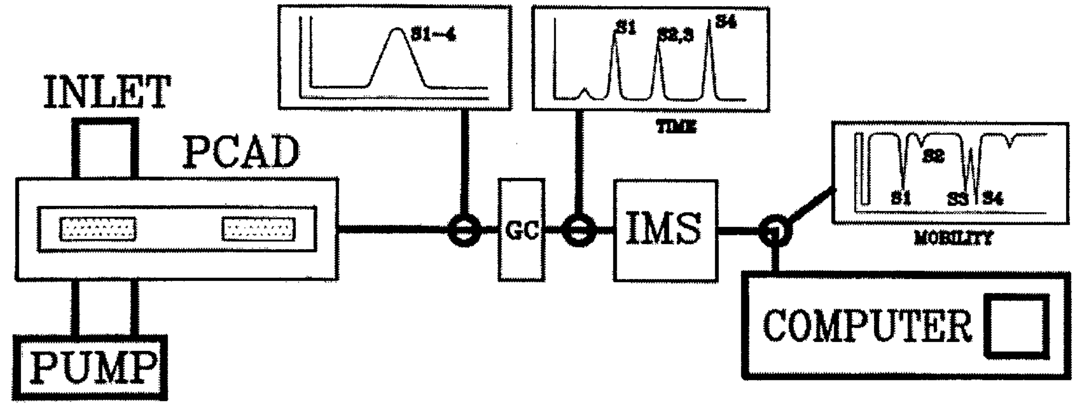
- Non-obtrusive passenger screening
- Uses Orion GC/IMS system
- High detection and throughput rate
- CCTV surveillance
- Remotely monitored

Vehicle Borne Explosive Detection System

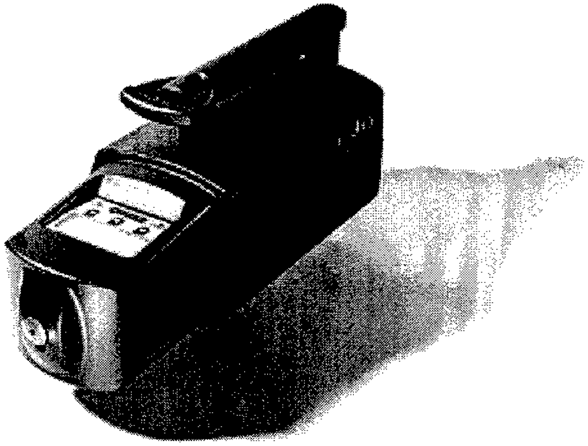
- Chemical sampling of vehicles
- Integrated CCTV and vehicle barriers
- Integrated weigh scale & database
- Remote command console
- Designed to site requirements
- Provides total control and risk management
- Containment system (optional)



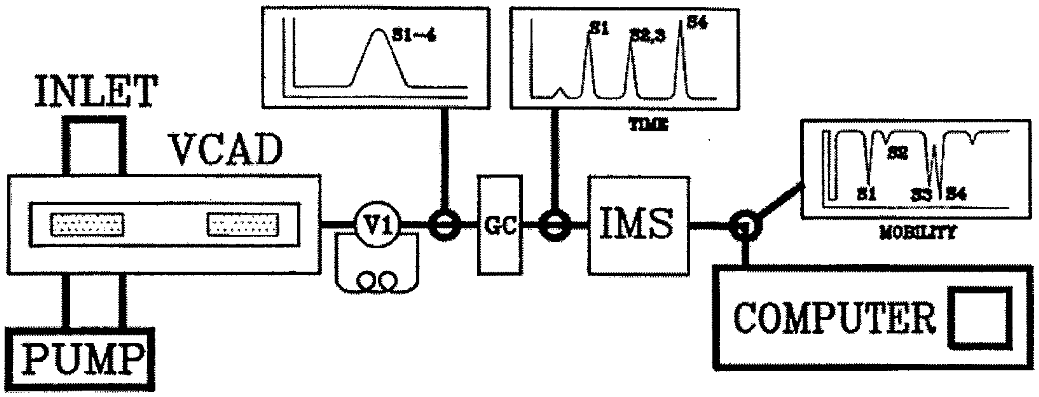
Northstar Handheld Drug Detection System



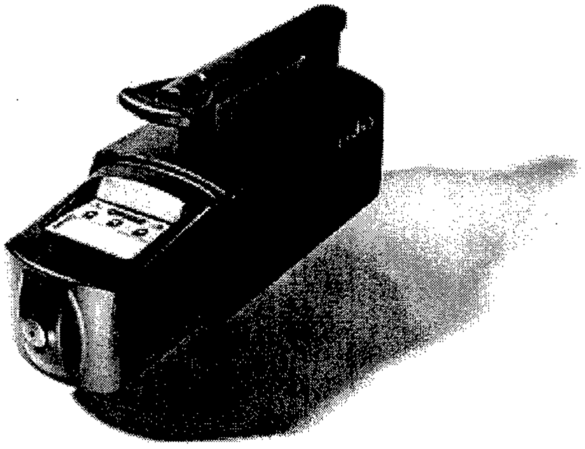
- 10 second analysis time
- Nanogram Sensitivity
- Cocaine, Heroin, THC, Methamphetamine
- GC-IMS Technology
- 12 vDC rechargeable lead acid battery
- 1 minute warm-up time
- Dimension: 16”L x 7”H x 6”W
- Weight: approximately 8lb (with battery)



Chemical Warfare Agent Detection System



- Configuration: Handheld
- Under 6 seconds analysis time
- Miosis Level Sensitivity
- Detection Targets: Nerve, Blister, Choking and Blood Agents
- GC-IMS Technology
- Power: Rechargeable battery
- Weight: approximately 12lb (with battery)



ids

Summary

- Fast GC-IMS technology can be configured to provide detection systems for many operational environments.
- Explosive, drug and explosive/drug detection systems are available.
- Walkthrough and vehicle explosive detection systems can be constructed.
- Also a handheld drug detection system has been developed.
- Additional configurations include a chemical warfare agent detector.

IDS Contact Info

Head Office

66 Slater Street, 6th Floor,
Ottawa, Ontario, Canada K1P 5H1
Tel.: (613) 230-0609 / Fax: (613) 230-3805

Operations Facility

152 Cleopatra Drive
Nepean, Ontario, Canada K2G 5X2
Tel.: (613) 224-1061 / Fax: (613) 224-2603

World Wide Web

www.idsdetection.com

CARGO SCREENING

Options from 450 kev to 10 Mev

EG&G ASTROPHYSICS

Things To Consider For Cargo Screening

- Goal
  - Verification
  - Interdiction
    - Type of Material
    - Amount of Material
- Type of Cargo
  - Size, density
  - Throughput

EG&G ASTROPHYSICS

Inspection Parameters

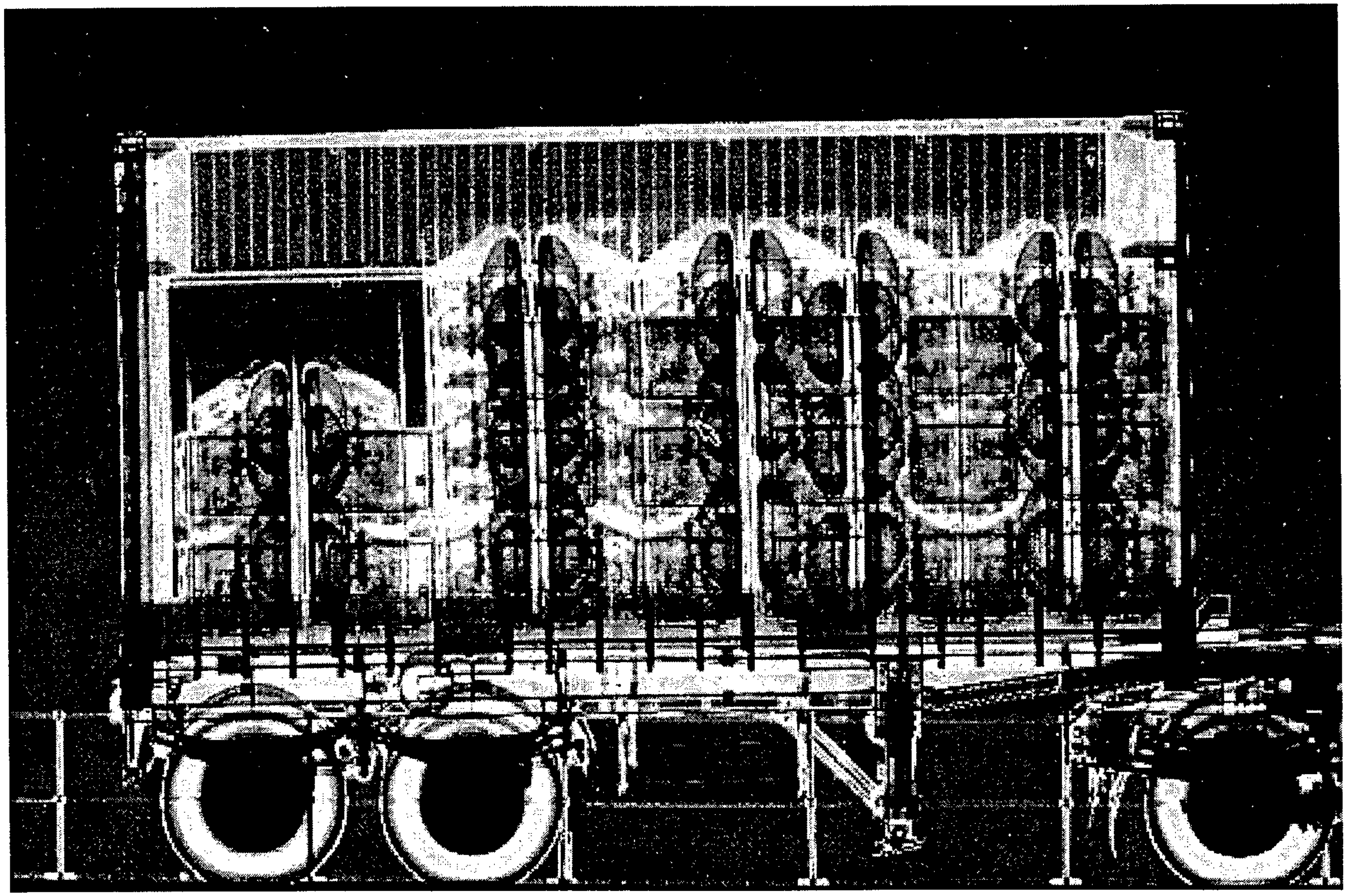
- Spatial Resolution
- Materials Resolution
- Penetration
- Operational Characteristics
  - Throughput
  - Number and training of operators
  - 100% or sampling

EG&G ASTROPHYSICS

Spatial Resolution

- 2 mm to 25 mm
  - 25 mm is adequate for very large objects
  - 2 mm is required for recognition tasks
- Cost of high resolution is very low
  - 10% of total system cost

EG&G ASTROPHYSICS

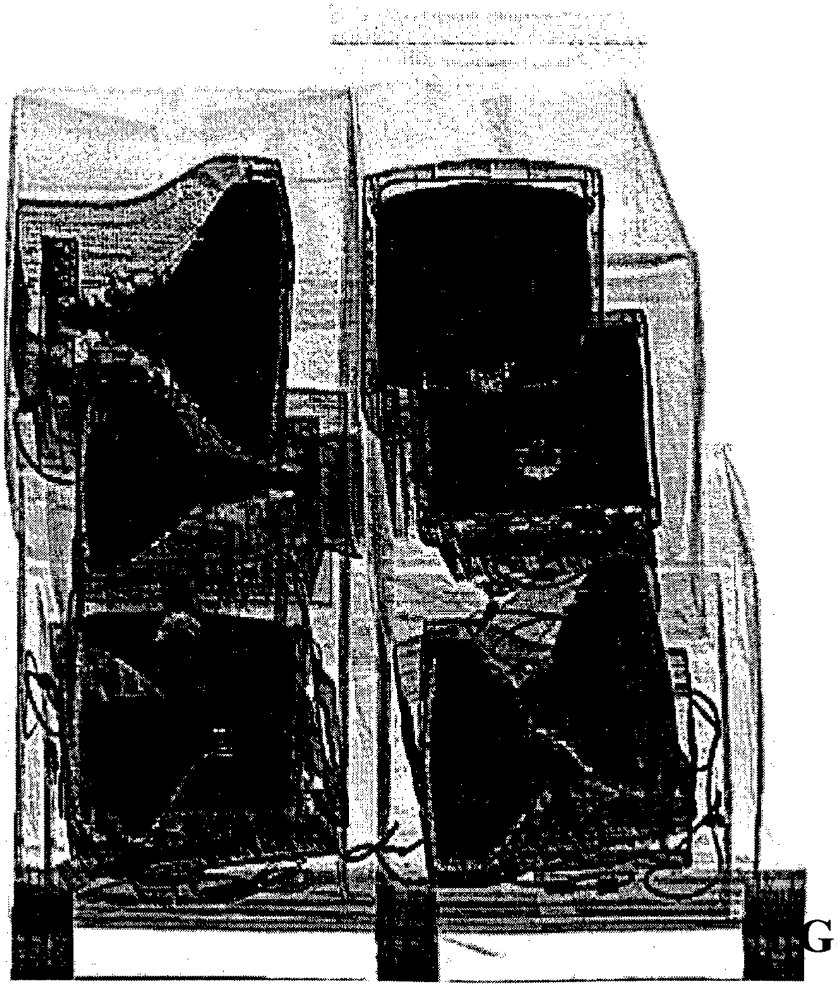


EG&G ASTROPHYSICS

Materials Resolution

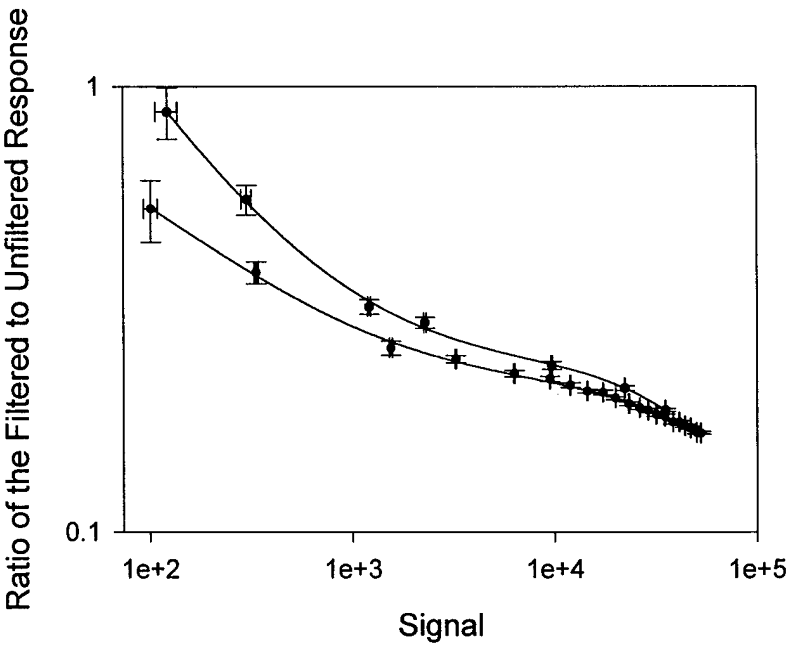
- Difficult for cargo
  - Limited at 450 keV
  - Available at 9 Mev
- Limited by physics
- Nuclear materials easily identified at 9 MeV
- Lucite and Iron easily identified at 9 Mev

E-Scan Image of Televisions (320KV)



G&G ASTROPHYSICS

Materials Discrimination using a Perspex Filter



400 mm Perspex

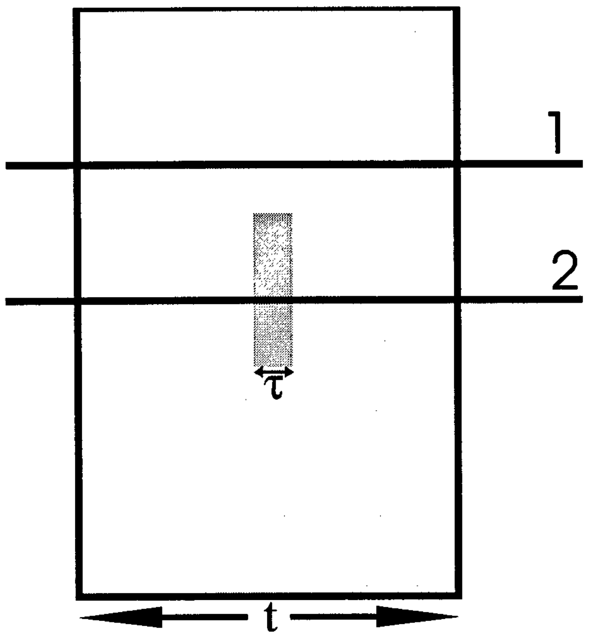
Figure 3

EG&G ASTROPHYSICS

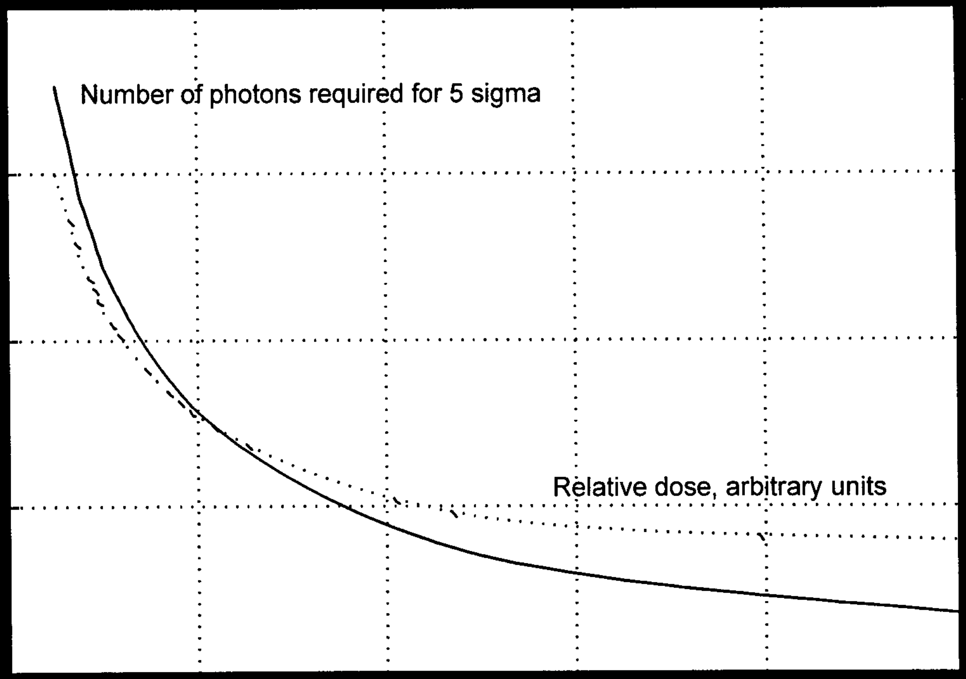
Penetration

- Why x-ray it if you can’t see what is inside
  - Bad guys quickly responds to system weaknesses
- Energy of x-ray depends on type of cargo
  - 450 good for pallet sized
  - 9 MeV superb for sea containers and trucks
  - 6 MeV for air cargo

IMAGING AT DIFFERENT HIGH ENERGIES

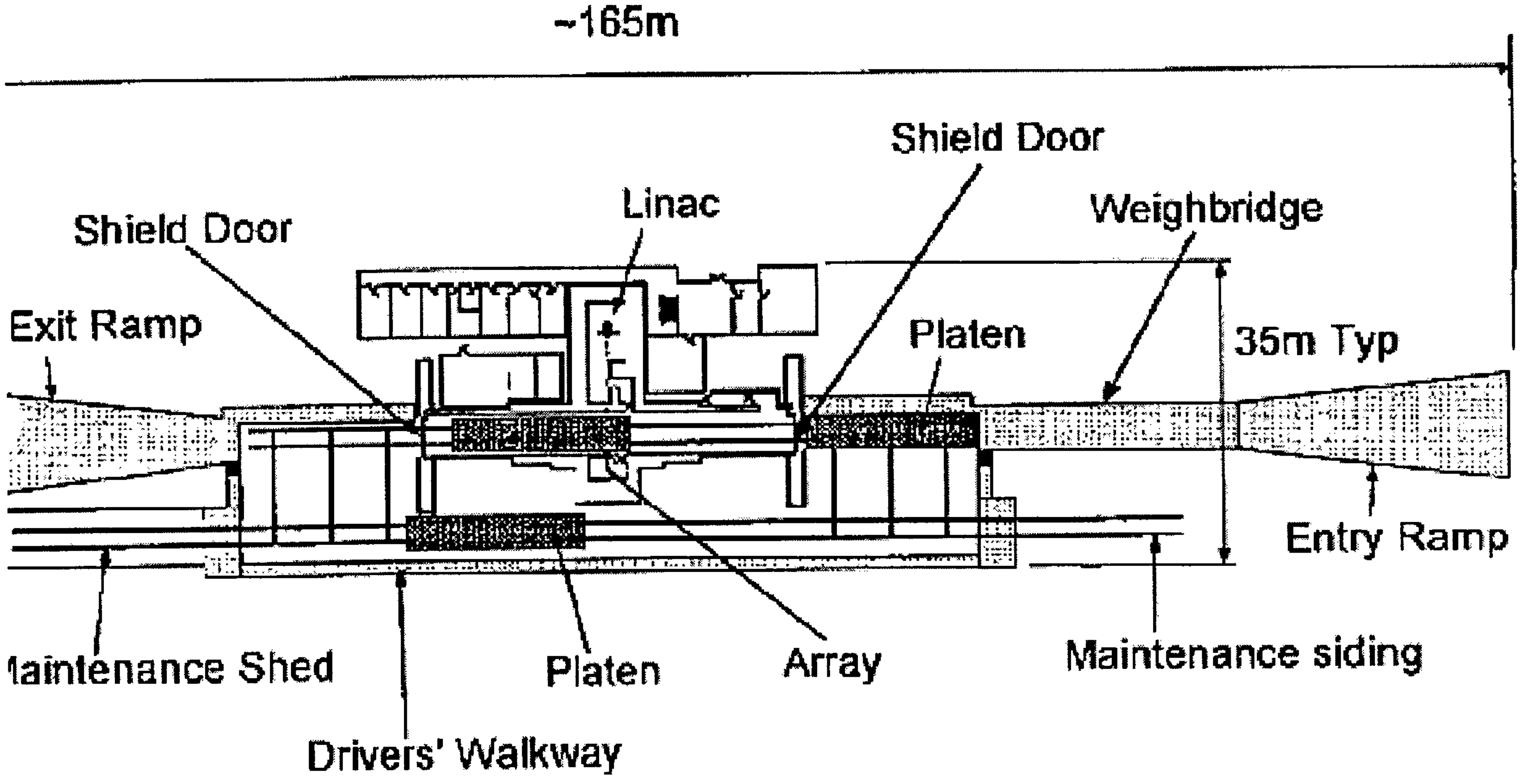


As a model we use the simple truck containg contraband in a smooth cargo

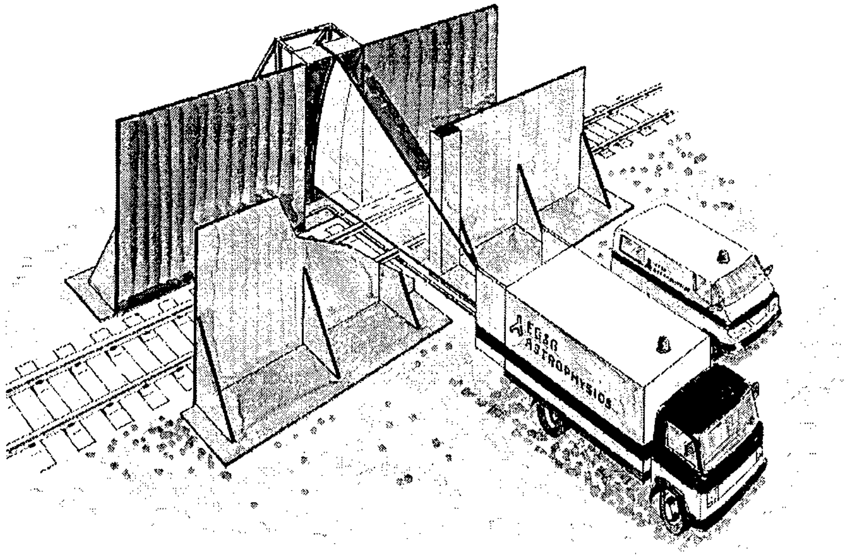

Number of photons required for 5 sigma
Relative dose, arbitrary units

Operational Characteristics

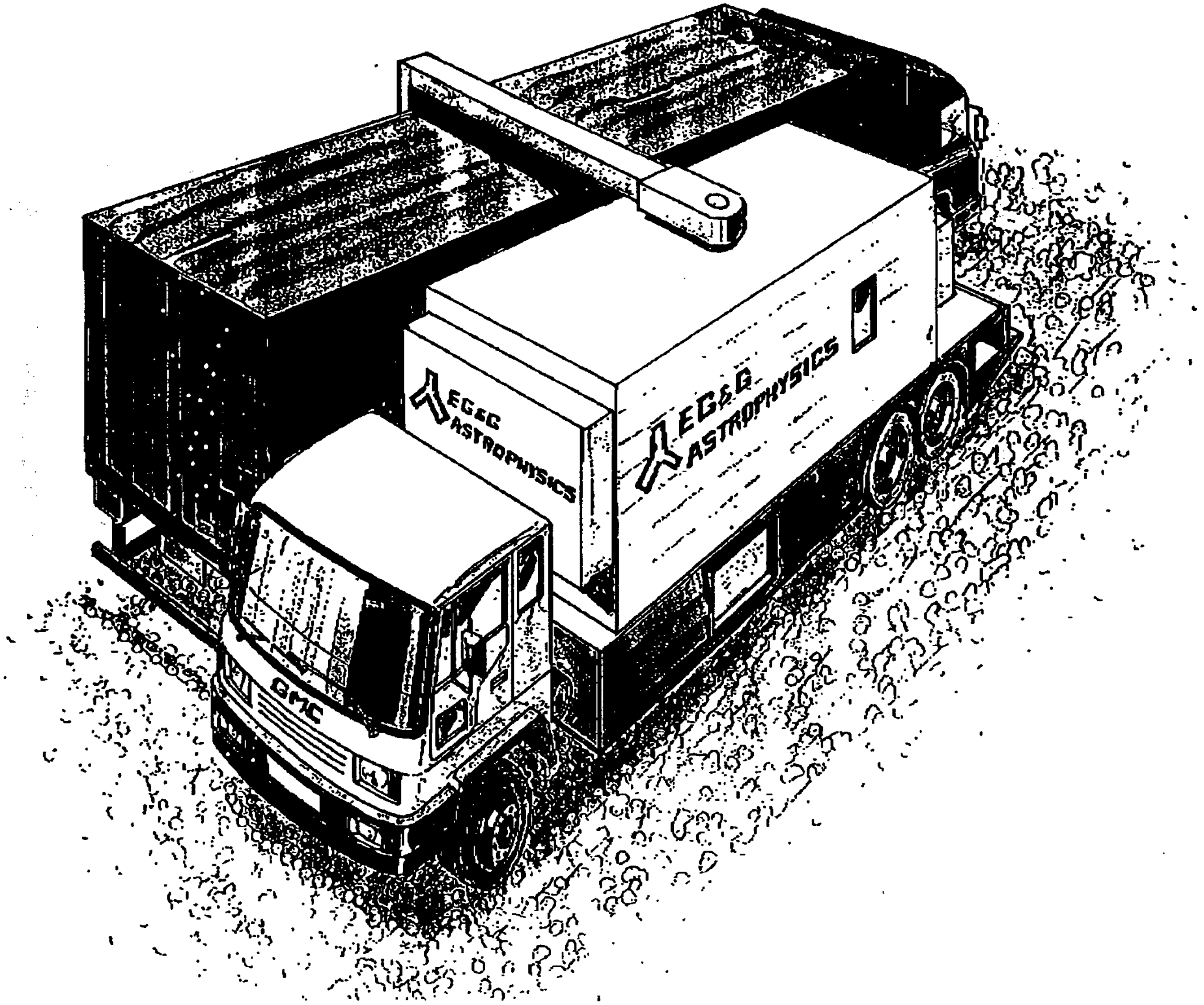
- Throughput
  - – 100% required for critical applications
  - – Intelligence led sampling
    - Intelligence plus x-rays improves detection
- Mobility
  - – Fixed site
  - – Relocatable
  - – Mobile


~165m
Shield Door
Linac
Shield Door
Weighbridge
Exit Ramp
Platen
35m Typ
Entry Ramp
laintenance Shed
Platen
Array
Maintenance siding
Drivers' Walkway

Train inspection system: Relocatable



EG&G ASTROPHYSICS



EG&G ASTROPHYSICS

Available from Astrophysics

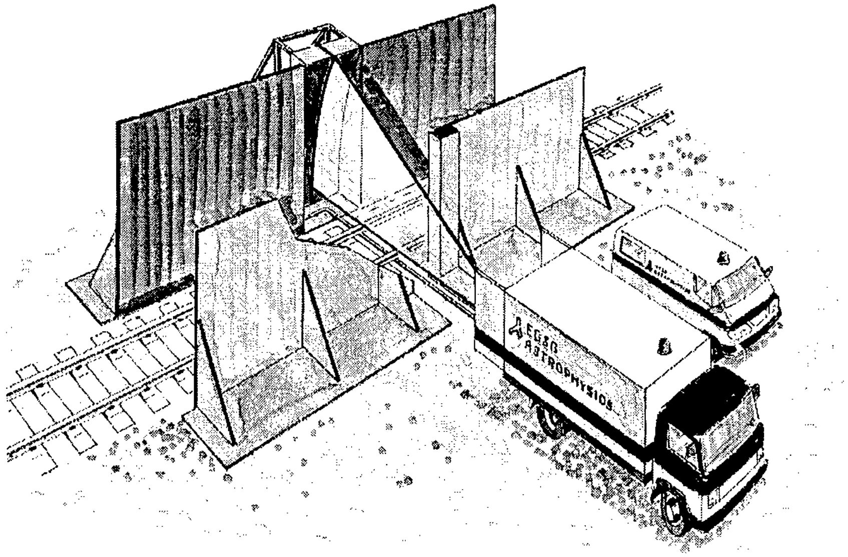
- 450 keV Backscatter/Transmission
  - Fixed site
  - Mobile
- 2 to 6 Mev Relocatable
- 6 to 9 MeV Fixed site

EG&G ASTROPHYSICS

2 to 6 MeV Relocatable System

EG&G ASTROPHYSICS

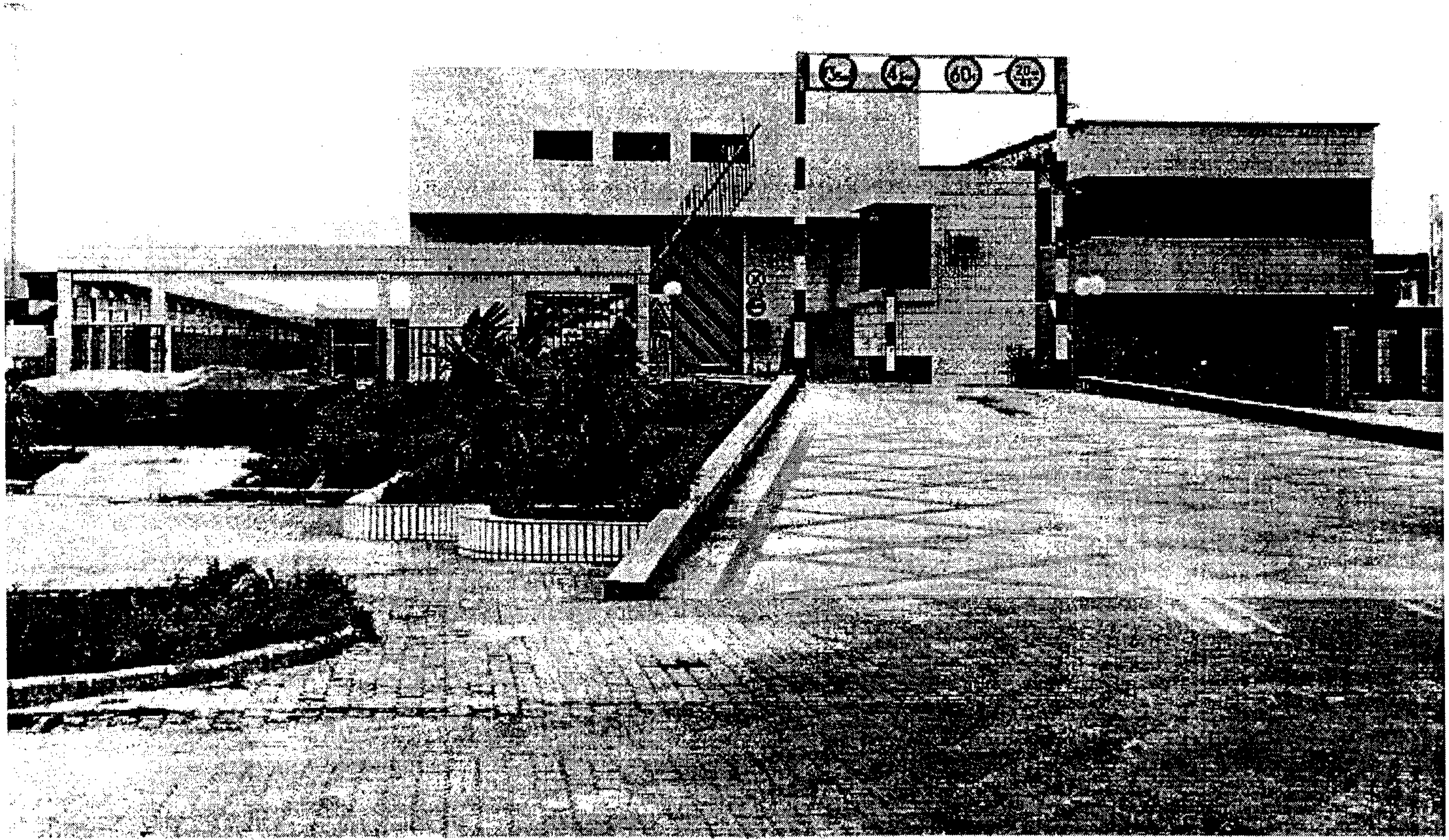
Train inspection system: Relocatable



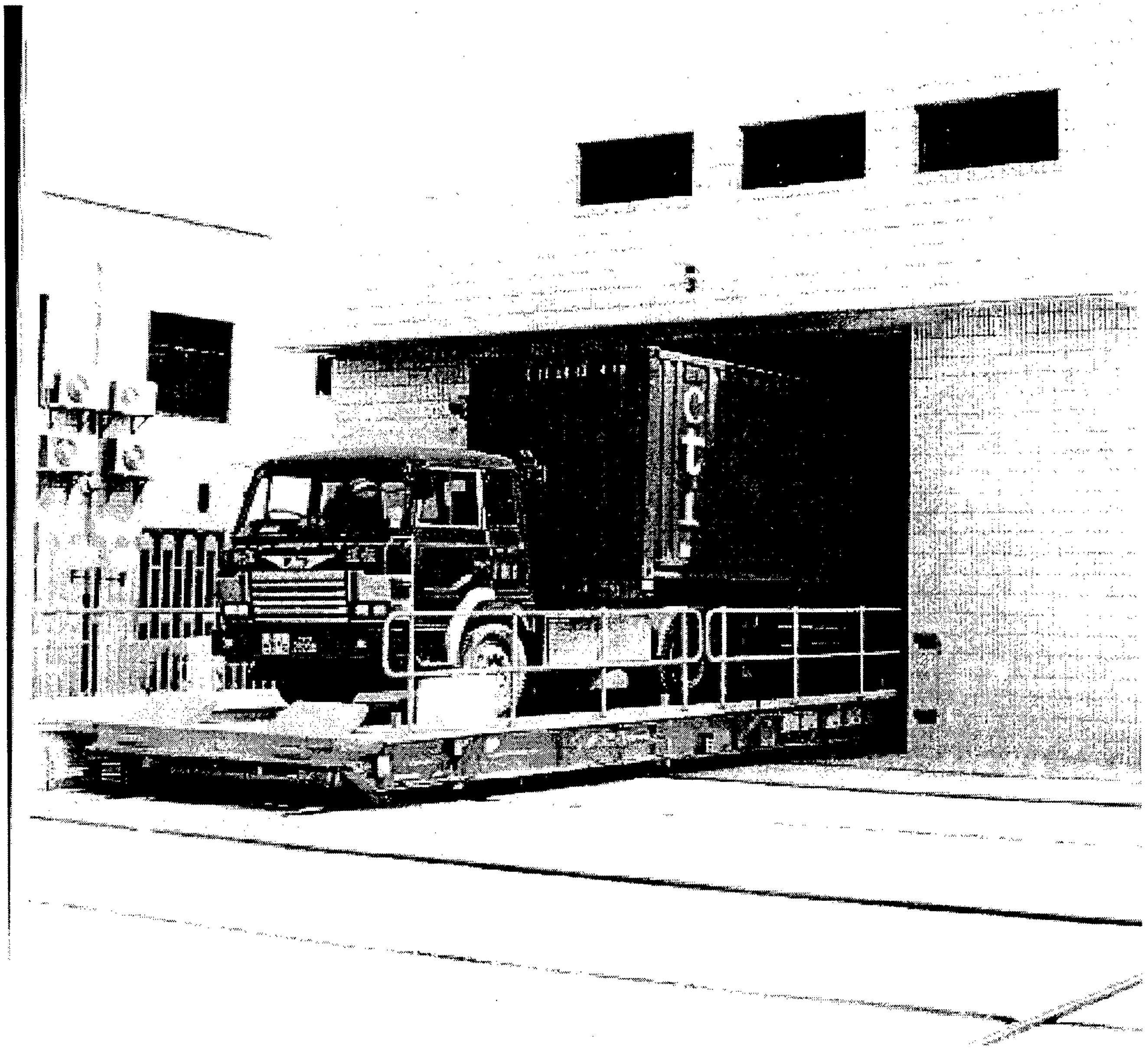
EG&G ASTROPHYSICS

9 MeV Fixed Site

EG&G ASTROPHYSICS

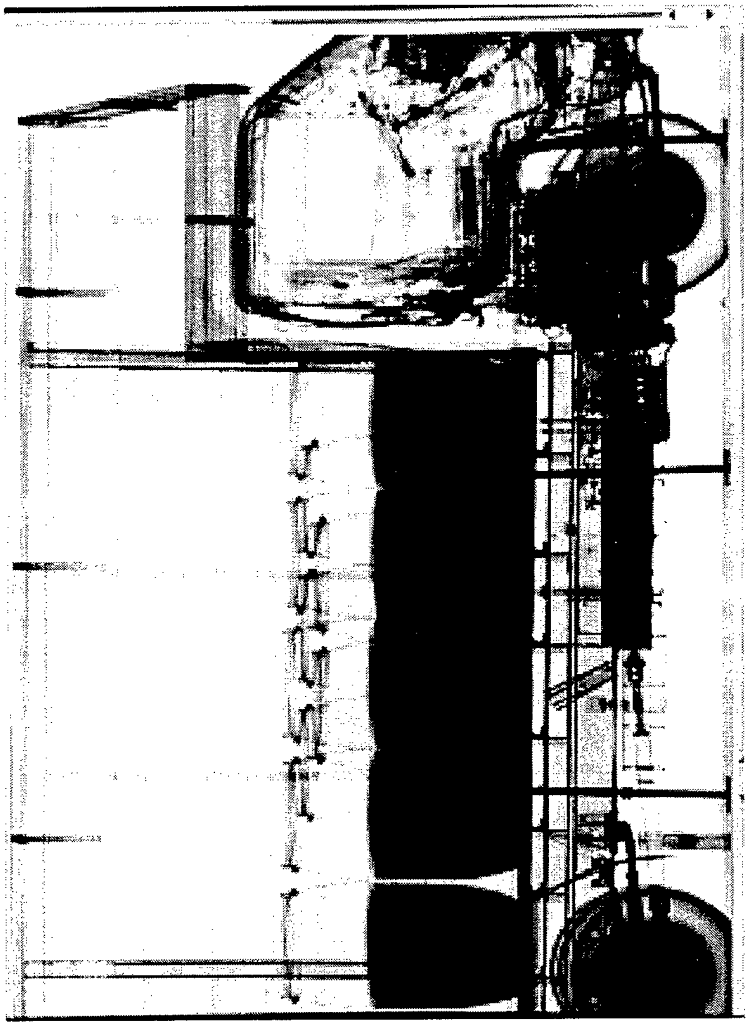


EG&G ASTROPHYSICS

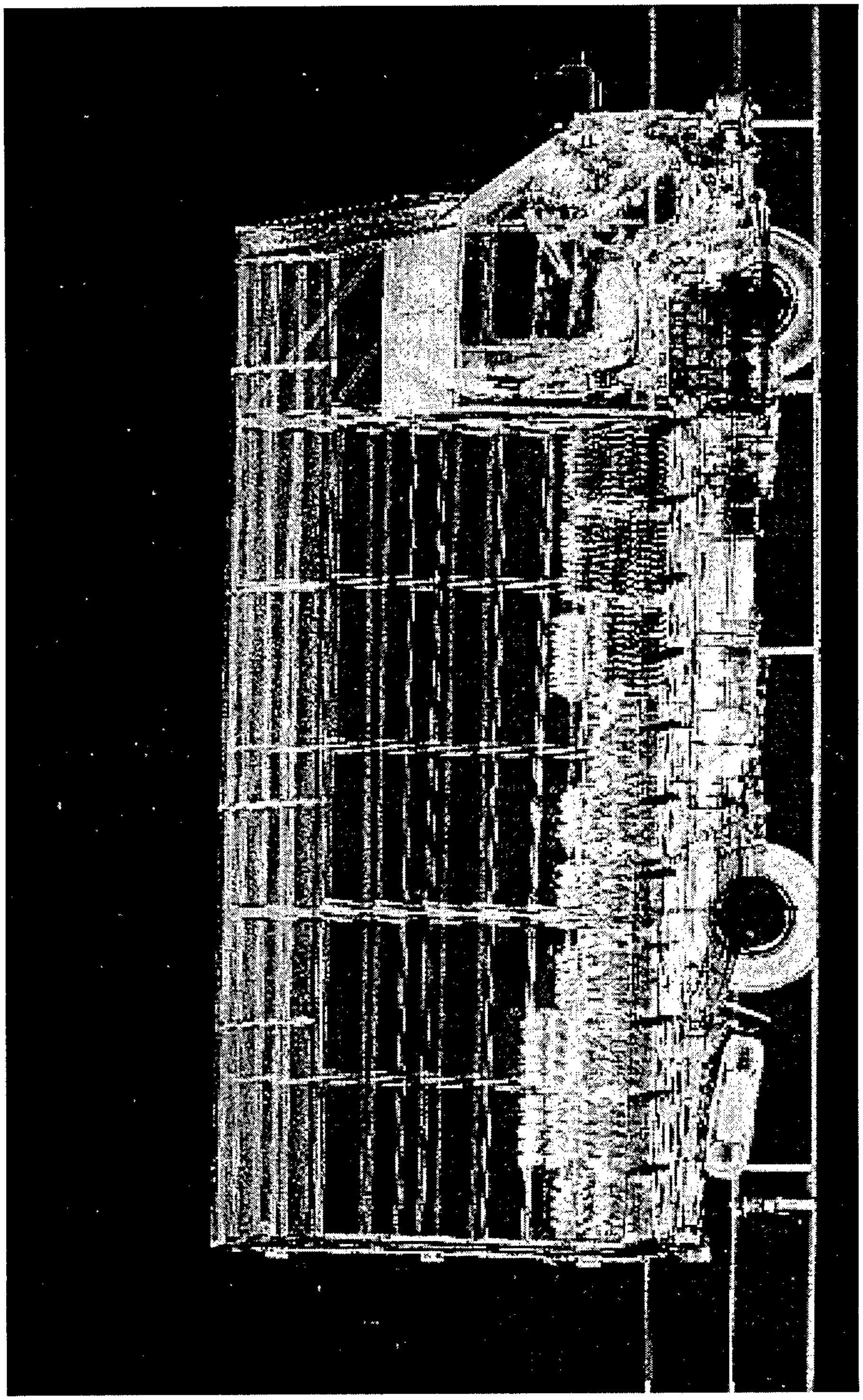


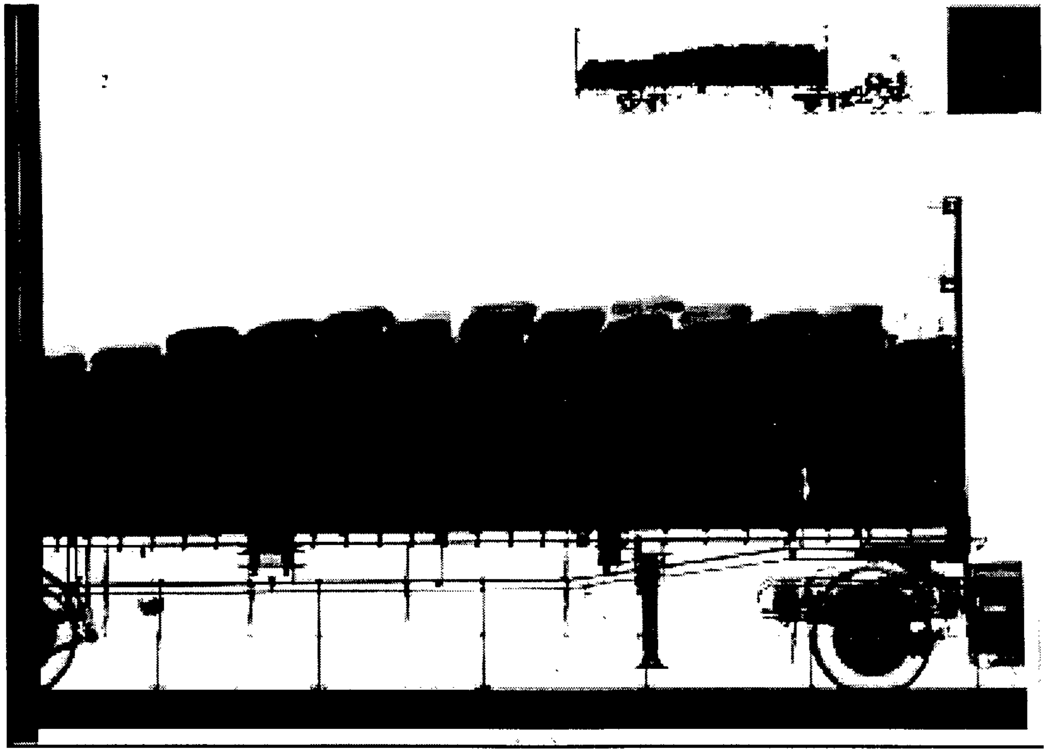
EG&G ASTROPHYSICS

EG&G ASTROPHYSICS



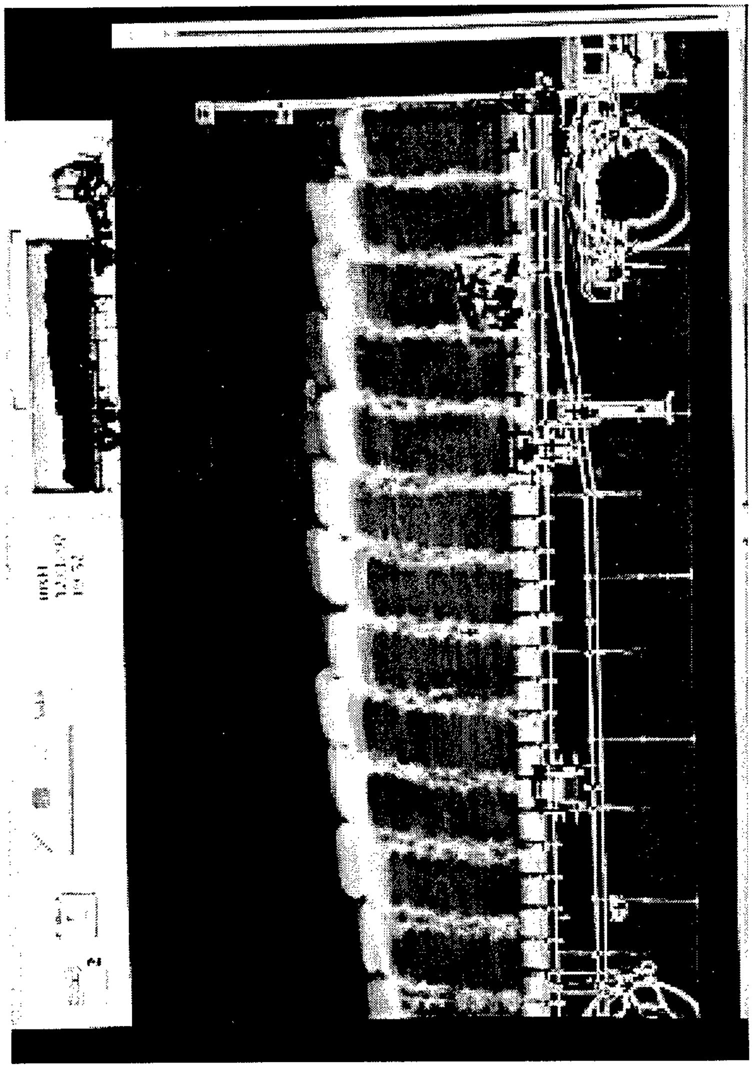
EG&G ASTROPHYSICS





EG&G ASTROPHYSICS

EG&G ASTROPHYSICS



M SCAN - NEW FEATURES

- MATERIALS DISCRIMINATION
- OPERATOR ANNOTATION
- HIGH RESOLUTION DISPLAY
- USES PROVEN IMAGING COMPONENTS
- NETWORKED OPERATOR REVIEW STATIONS

EG&G ASTROPHYSICS

Tactical Automated Security System (TASS)

First Operational Deployment

Mr. Jim Norman

6/16/98

TASS Background

- 25 June 1996 - Khobar Towers bombing
- AF Chief of Staff mandates that Force Protection is an "Urgent and Compelling Need"
- Electronic Systems Center awards TASS production contract to TRW
  - 4 days from solicitation to award)

Fast Track Performance

- 100 days after award, TRW and AlliedSignal team on the ground in Southwest Asia
- 104 days after contract award, TRW ships first equipment to Kuwait
- 30 tons of equipment in-country within 125 days of contract award

Team TASS
TACTICAL AUTOMATED SECURITY SYSTEM

What is TASS?

TRW

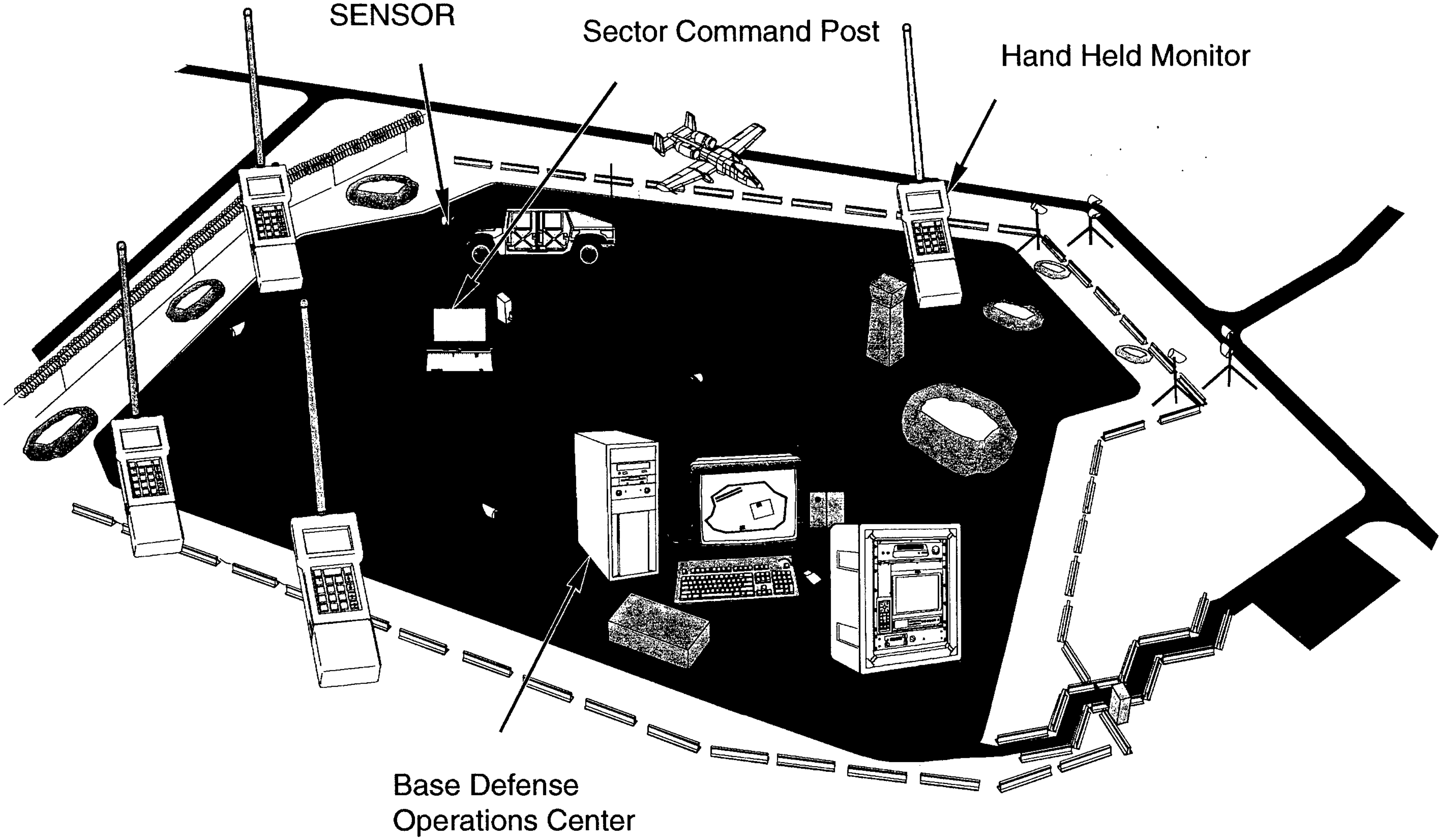
- TASS is an advanced intrusion detection and assessment security system
- TASS is modular, portable, relocatable, and self powering
- Employs a variety of sensors...Microwave, Infrared, Magnetic, etc
- Alarm data is transmitted via RF or hardwire

Products
& Services

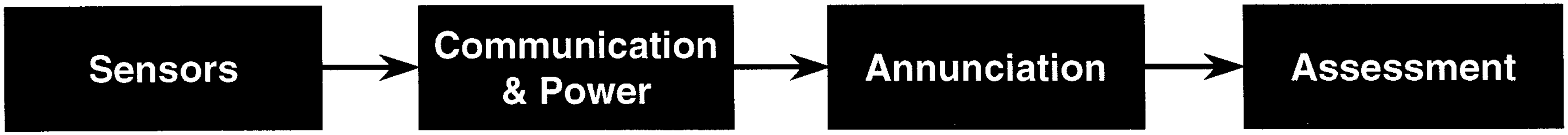
What is TASS ? Cont.

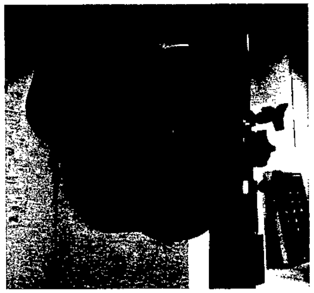
- Sensors and RF transmitters are powered by either solar panels, battery, or AC current
- Desktop & laptop computers, and hand-held monitors receive, process, and display alarms
- Map displays are geographically correct with multiple overlays possible
- Hand-Held, vehicle mounted, and wide area surveillance thermal imagers assess alarms

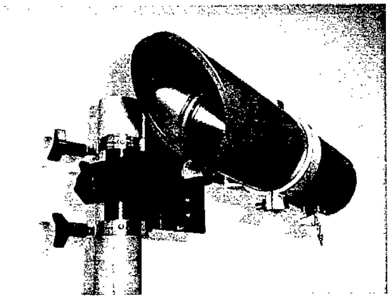
Typical Airbase Installation

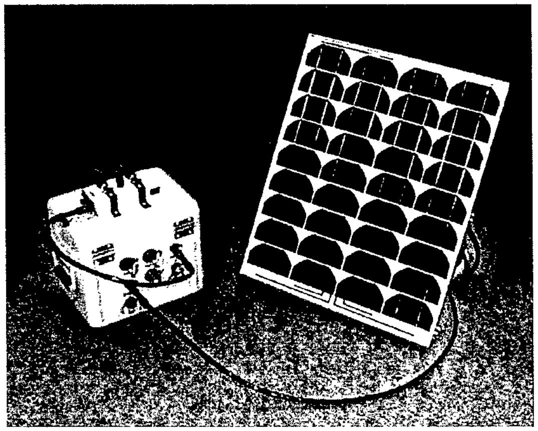


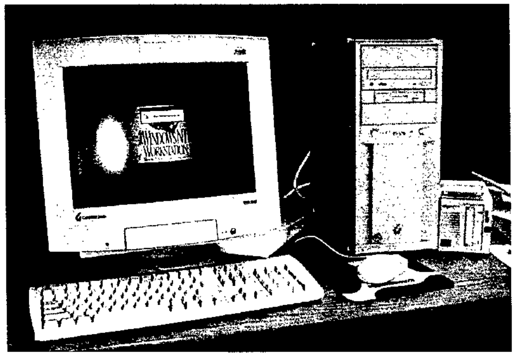
Intrusion Detection Functions

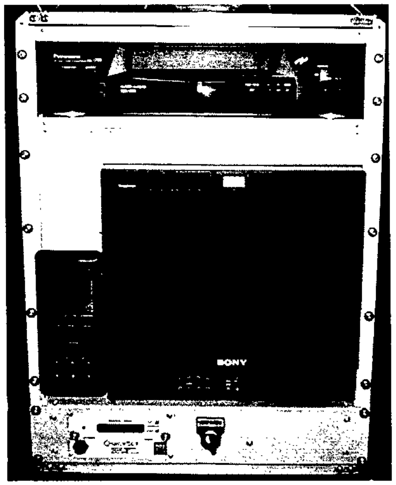

Sensors → Communication & Power → Annunciation → Assessment





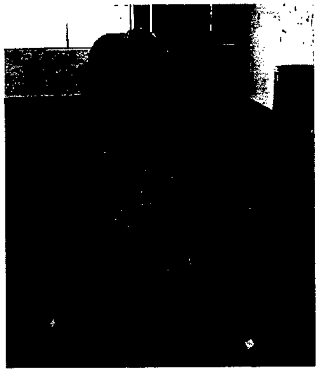
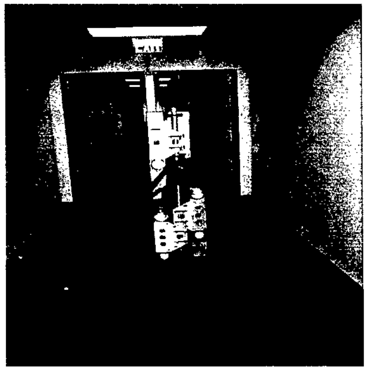
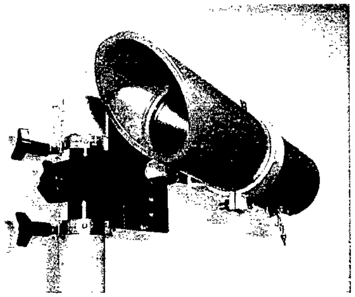






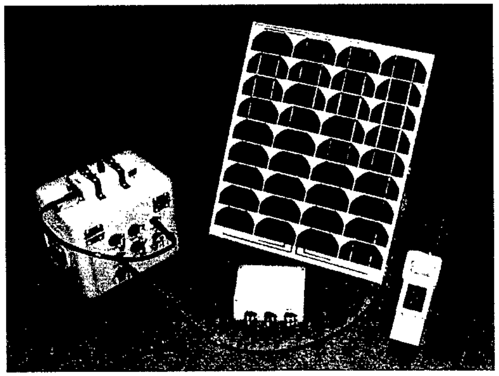
Sensors

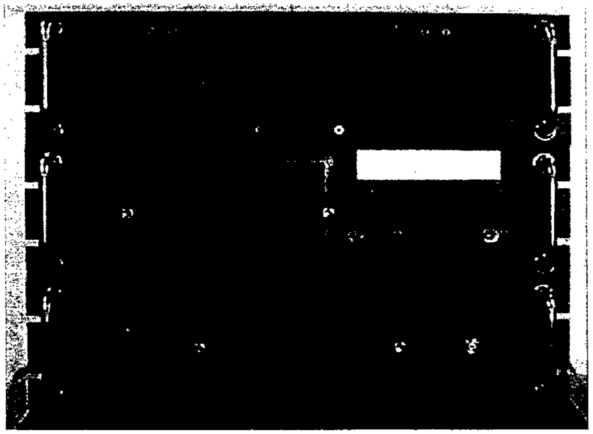
Sensor Types	Detection	Application
Monostatic Microwave	Motion	Perimeters: base, flightline, housing, storage areas,
Bi-Static Microwave	Motion	Same
Active Infrared	Beambreak	IR Fence
Passive Infrared	Heat	Gaps, approach avenues
Tactical	Various	Avenues, trails

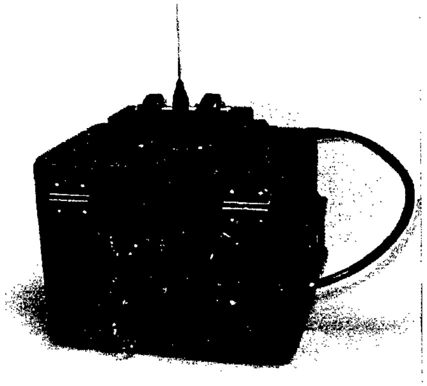




Comm & Power

Components	Function
Rechargeable Battery Module	Powers 1-2 sensors & CM, formats alarm and health messages, charges batteries (110/220v AC or solar panel)
UPS	Uninterruptible power for annunciators
Comm Module	Radios alarms & health to control center Can be polled for state-of-health

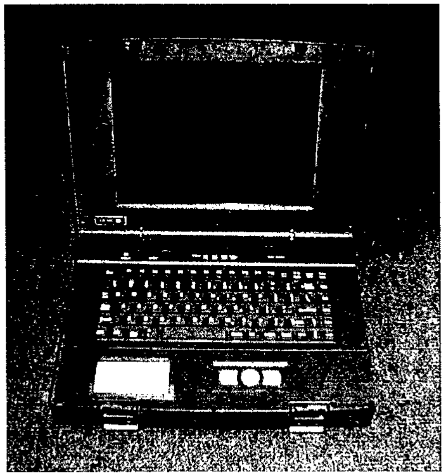


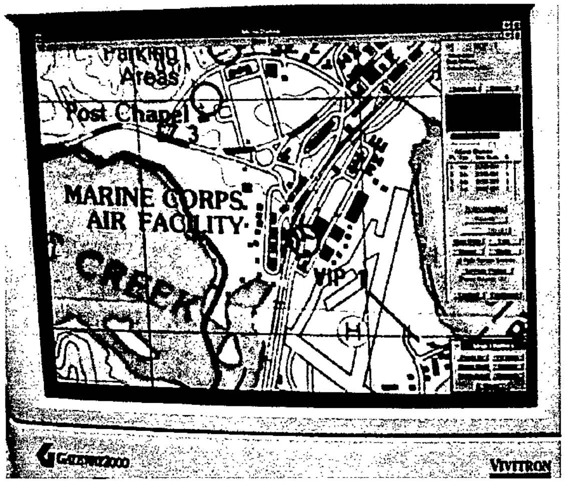


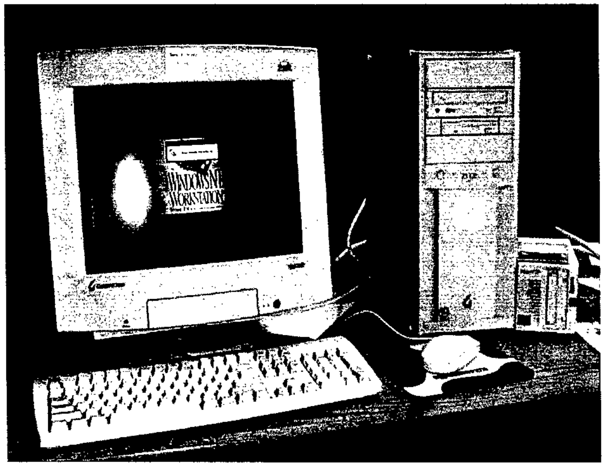


Annunciation

Components	Function
Hand-Held Monitor (HHM)	Receives/displays alarms (text only), programs Comm Modules
Laptop Annunciator Desktop Annunciator	Computers with graphical display of base map, sensor locations, alarm and health status, alarm history. Laptop is ruggedized.

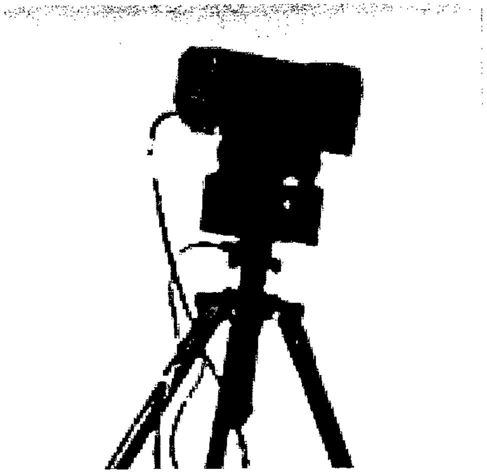


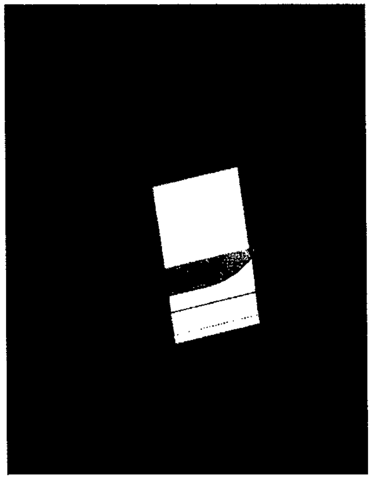




Assessment

Components	Function
Hand-Held Thermal Imager	Hand-Held, battery operated TI for use in patrols, stationary positions, etc
Short-Range Thermal Imager	Vehicle- or pole-mounted for 0.5-1 km
Wide-Area Surveillance Thermal Imager	Tower or tripod mounted TI with range to several kilometers





Southwest Asia Installations

- ➡ Saudi Arabia
    - ➪Prince Sultan Air Base, Eskan Village, Taif
    - ➪370 sensor suites; 20,000 meter perimeter
- ➡ Kuwait
    - ➪Al Jaber & Ali AL Salem Air Bases
    - ➪110 sensors suites; 7500 meter perimeter
- ➡ UAE
    - ➪Al Dhafra Air Base
    - ➪40 sensors suites; 3000 meter perimeter

Global Installations

- ➡ Ground Based Radar Sites
- ➡ Operation Bright Star
  - ⇨Cairo West Air Base, Egypt
- ➡ Air Expeditionary Forces
  - ⇨Shaikh Isa Air Base, Bahrain

Installation Highlights

- Commercial-Off-The-Shelf (COTS) worked!
  - Temperatures exceeded manufactures specs by >25 degrees
  - Reliability proved better than advertised
- TRW & AlliedSignal worked!
  - Met critical needs of the customer under adverse conditions
  - Lived and worked side-by-side with our customers
  - Overcame challenging obstacles in real time
- Living with the customer provided instant coordination and invaluable insight
  - Teamwork, a common knowledge base

Products
& Services

Installation Highlights, cont.

- Early site surveys substantially increase efficiency
  - Buy only what you need; bring everything that you need
  - Identify site preparation requirements
- On site support smoothes the transition period
  - Big paradigm shift: new methods, new technology, new logistics
- Training is critical
  - Train operators and trainers, of course
  - But also system managers, logisticians and command section
    - » Fundamental changes to the way you do business

Installation Highlights, cont.

- There will always be surprises
  - Customs, visas, religion, taxes, site prep, landmines
  - Bring an experienced crew, roll with the punches
- Contracts can be brought in on time and within budget

Kudos

- ➡ Electronic Systems Center
- ➡ USAF Security Forces Air Staff
- ➡ Air Combat Command
- ➡ CENTAF
- ➡ USAF Security Forces Battle Lab
- ➡ AlliedSignal Technical Services

Total Teamwork => Success

Points of Contact

- ➡ Jim Norman

  TRW
  1800 Glenn Curtis St
  DH4/1131
  Carson, CA. 90746
  310-764-312 or e-mail Jim.Norman@TRW.com

- ➡ Jay Brossier

  TRW
  1800 Glenn Curtis St.
  DH4/1131
  Carson, CA. 90746
  310-764-6554 or e-mail Jay.Brossier@TRW.com

CW Sentry

Installed Chemical Agent Detector for Building Security

Presented at

14th Annual Security Technology Symposium and Exhibition

Williamsburg, Virginia
June 15-18, 1998

by

N. Lynn Jarvis

Microsensor Systems. Inc.
62 Corporate Court
Bowling Green, KY 42103
(502) 745-0099

CW Sentry: Installed Chemical Agent Detector for Building Security

Security Requirement:

It was vividly demonstrated in Japan that organized, well funded terrorist groups are fully capable of delivering and releasing lethal quantities of chemical agents at sites of their choice. As sites for such terrorist attacks will almost certainly be locations with relatively uncontrolled access by large numbers of people, it may be extremely difficult to detect carefully packaged and concealed agent prior to release. Even in the absence of prior detection, the security of a site or facility, and the safety of its people, will be critically dependent on the rapid detection of any agent released.

Whatever the facility or building selected by terrorists for an attack - a subway platform, building lobby, or entrance to a sports arena - the spread of the deadly gas, and thus its lethal effect, will largely be controlled by movement of air within the structure, i.e. by the ventilation system.

Safety and security of the building, therefore, requires that an Installed Chemical Agent Detection System must:

- be capable of rapid, highly reliable detection and alarm
- be capable of continuous, unattended operation
- have very low probability of false alarms
- be strategically located to provide the earliest possible warning
- be interfaced with HVAC systems for automatic shutdown
- provide complete building coverage

CW Sentry

Design Concept

The CW Sentry was designed to include the same solid-state sensor "engine" as used in the successful SAW Miniature Chemical Agent Detector (SAW MINICAD). The heart of the detector module is an array of surface acoustic wave devices optimized for the simultaneous detection of both nerve and blister agents at low concentrations. The sensors respond within 60 seconds to a vapor challenge and, as they are reversible, can provide an ALL CLEAR as well.

The CW Sentry package, as shown in Figure 1, is both compact and rugged, and can be easily installed for fixed site operation. The instrument was designed with an automatic switch closure for easy interface with an HVAC system and/or an alarm panel. As the SAW sentry must operate automatically, continuously and reliably over extended periods of time, it was designed with many self-diagnostic and back-up features. It has an onboard computer that can be programmed to notify maintenance personnel when service is required. It has a modular design in which each component can be easily and quickly replaced in order to minimize maintenance. Another design objective was to keep the cost as low as possible.

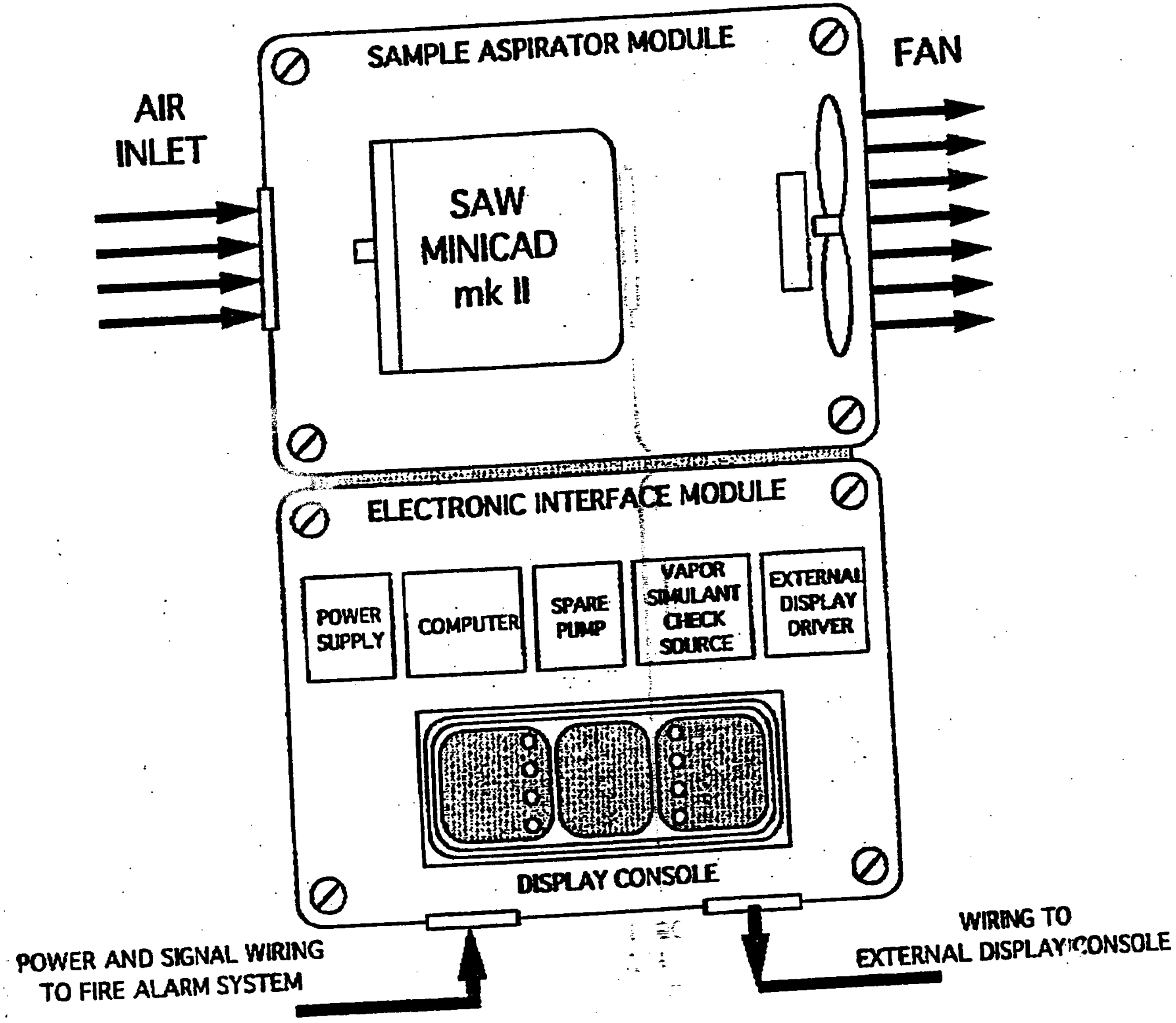

SAMPLE ASPIRATOR MODULE
FAN
AIR INLET
SAW MINICAD mk II
ELECTRONIC INTERFACE MODULE
POWER SUPPLY
COMPUTER
SPARE PUMP
VAPOR SIMULANT CHECK SOURCE
EXTERNAL DISPLAY DRIVER
DISPLAY CONSOLE
POWER AND SIGNAL WIRING TO FIRE ALARM SYSTEM
WIRING TO EXTERNAL DISPLAY CONSOLE

Figure 1. Schematic Diagram of CW Sentry Installed Chemcial Agent Detector

Key Design Features

One of the features of the CW Sentry design is that it has a built-in air pump capable of pulling samples from locations up to 25 feet away. The Sentry can sample from four locations simultaneously and alarm within 60 seconds. For ease of installation and maintenance, the system was designed to operate at standard 24 volt DC fire alarm power, thus it can interface easily with remote monitoring consoles or other alarm panels. It is, in fact, designed to interface readily with standard fire alarm systems via a relay switch closure. Another key feature is the inclusion of an onboard vapor check source. This is one of self diagnostic features of the instrument that permits it to routinely determine that the sensors and identification algorithm are functioning properly and providing the required detection capability.

The CW Sentry also was designed with the option for remote control and alarm via an RS 232 serial data port. Remote console alarm panels can be installed in critical or highly sensitive areas such as VIP offices, conference rooms or an auditorium where rapid evacuation might be desired. The overall system was designed for easy installation and operation with little required training.

SAW Sensor Module

The SAW sensor module in the CW Sentry has two active surface acoustic wave (SAW) resonator devices for detection and a third for reference purposes. One active resonator has a coating selective for the nerve agents (GD, GB, GA) and the other a coating selective for mustard (HD). A typical device is shown below in Figure 2.

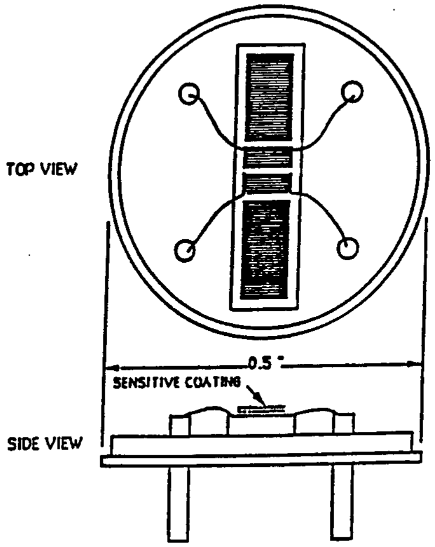


Figure 2. SAW Resonator Device used in CW Sentry Chemical Agent Detector

Identification of the agents is made by a computer controlled algorithm that analyzes the vapor response of the sensors. Typical sensor array response to a challenge of 1 ppm GA is shown in Figure 3. The algorithm measures and analyzes such features as time response, relative peak heights, rate of rise, and other peak features. The computer then compares the measured features with data stored in memory. Based on the comparison, the computer will decide whether or not the detected vapor is a chemical agent and its relative concentration. Before and after each run a baseline signal is determined.

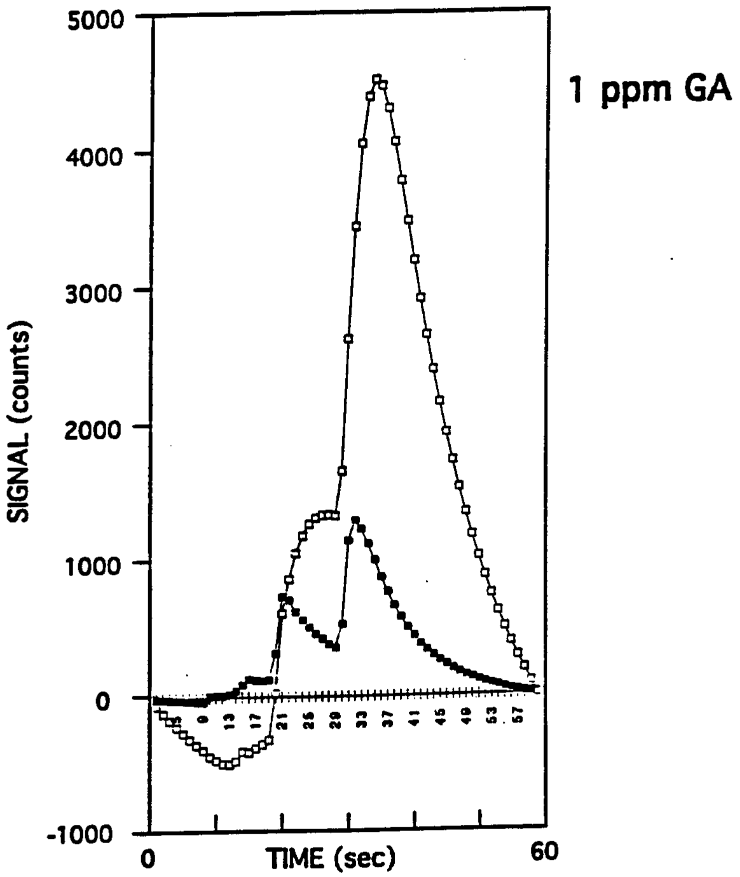
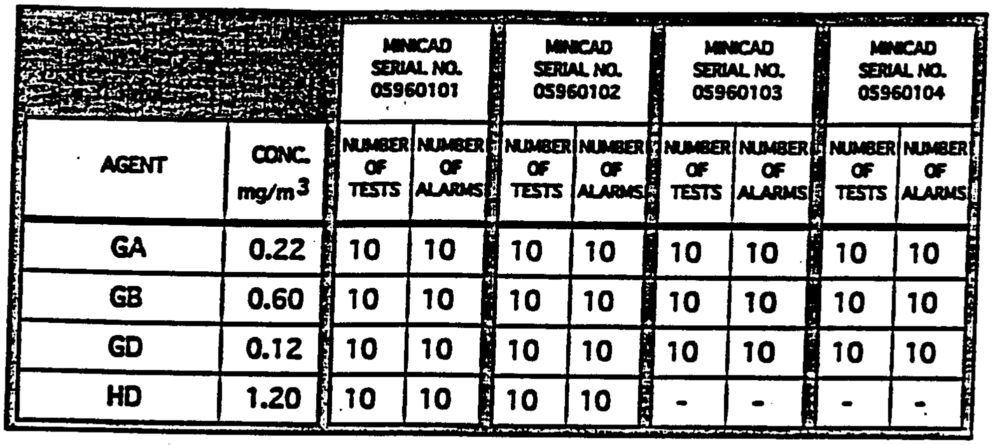


Figure 3. SAW Sensor Response to 1 ppm GA

The SAW sensor module as used in the SAW MINICAD and the CW Sentry has been extensively tested with both nerve agents and HD. The test results, shown in the accompanying Figure 4, were conducted at GEOMET Technologies, Inc. and were verified by MINICAMS gas chromatographic analysis. Four different MINICAD instruments were tested with GA, GB, GD, and HD at concentrations close to the desired instrument alarm levels. These levels are well above the actual instrument detection limits, which greatly decreases the likelihood of either a false negative or a false positive readings. Each of the four MINICAD instruments was exposed to each vapor a total of 10 times, and in each case the instrument alarmed as required. No false negatives were observed at any time.



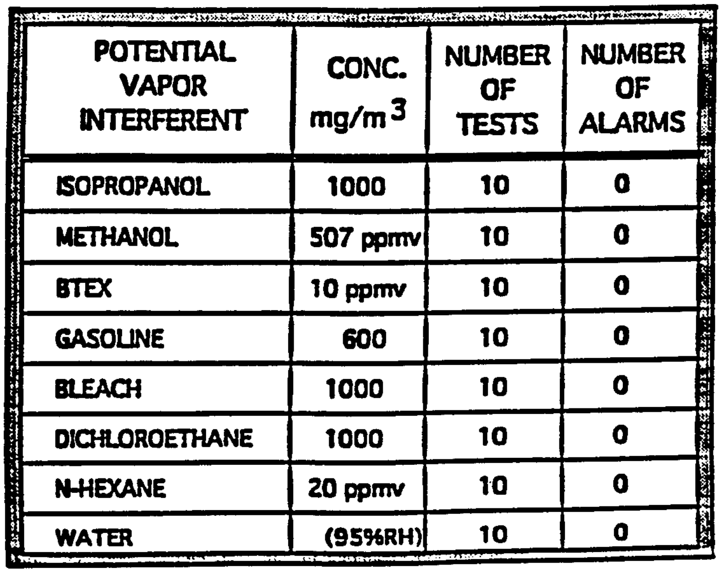
		MINICAD SERIAL NO. 05960101		MINICAD SERIAL NO. 05960102		MINICAD SERIAL NO. 05960103		MINICAD SERIAL NO. 05960104	
AGENT	CONC. mg/m^3	NUMBER OF TESTS	NUMBER OF ALARMS	NUMBER OF TESTS	NUMBER OF ALARMS	NUMBER OF TESTS	NUMBER OF ALARMS	NUMBER OF TESTS	NUMBER OF ALARMS
GA	0.22	10	10	10	10	10	10	10	10
GB	0.60	10	10	10	10	10	10	10	10
GD	0.12	10	10	10	10	10	10	10	10
HD	1.20	10	10	10	10	-	-	-	-

* CW agent exposure testing conducted at GEOMET Technologies, Inc. , Germantown, MD on January 3-5, 1996.

** All CW agent vapor concentrations verified by MINICAMS gas chromatographic analysis.

Figure 4. SAW Sensor Performance With CW Agents

Several companion studies have also been made of the response of the SAW sensor modules to potential interferent vapors. The test summarized in Figure 5 was one in which the concentrations of the potential interferents were determined. In these tests nine common interferent vapors were used, including, alcohols, gasoline vapors, a chlorinated solvent, water and an alkane, at the concentrations noted. In ten separate tests with each vapor no false alarms were observed. In more severe tests, in which vapors near their saturation concentrations were used, SAW MINICADS were exposed to nearly 100 different chemical vapors with excellent interference rejection. Interference was only observed for a few compounds, and then only at concentrations many thousands of time greater than the agent alarm values.



POTENTIAL VAPOR INTERFERENT	CONC. mg/m^3	NUMBER OF TESTS	NUMBER OF ALARMS
ISOPROPANOL	1000	10	0
METHANOL	507 ppmv	10	0
BTEX	10 ppmv	10	0
GASOLINE	600	10	0
BLEACH	1000	10	0
DICHLOROETHANE	1000	10	0
N-HEXANE	20 ppmv	10	0
WATER	(95%RH)	10	0

Figure 5. Interference Rejection by SAW Sensors

CW Sentry Specifications

The specifications of the CW Sentry are summarized in the following table:

CW SENTRY SPECIFICATIONS

Weight:	6 pounds
Size:	4" x 6.25" x 9.5"
Enclosure:	Die-Cast Aluminum
Sensor System:	Surface Acoustic Wave Microsensors
Alarm Thresholds:	0.1 mg/m3 GD 0.2 mg/m3 GA 0.5 mg/m3 GB 1.0 mg/m3 HD
Response Time:	60 Seconds
Maintenance Interval:	5,000 hours
Power Required:	24 Volts DC @ 3A
Alarms:	(Four, Normally Open Switch Closure) 1 - Nerve Agent 2 - Blister Agent 3 - High Concentration 4 - System Fault
Data Output:	(Optional RS232C serial ASCII)
Operating Temp:	+5°C to +45°C
Humidity:	0% to 95% RH, non-condensing
Warranty:	One year or 5,000 hour of use (parts and labor)

Technical Approach for CW Sentry Implementation

Prior to installation of a SAW Sentry Installed Chemical Agent Detector, a careful assessment should be made of the chemical threat vulnerability of the selected facility. This would include an assessment of both internal and external factors such as concentration and movement of people, points of ingress and egress, location external air intakes, actual or potential crowd control points, and the many other factors that contribute to a facilities vulnerability to a chemical attack.

Special attention should be given to surveying the engineering facilities of the building, which would include review of appropriate drawings and discussions with facility management and engineers. It will be necessary to determine whether that the CW Sentry alarm system can be readily interfaced with existing HVAC fans and shutters so as to quickly shut down air movement within the facility in the event of a chemical attack, or if some modification will be needed. A review of the current fire alarm, or other special alarm systems and alarm consoles will also be required.

Based on the results and analysis of the facility surveys, a decision can be made as to where the CW Sentry units should be installed and how best to interface the units with existing facility equipment. Installation and testing of the CW Sentry could then proceed, including training of building engineering and security personnel on the use and maintenance of the system.

Summary of CW Sentry Features

Security Requirements

- Rapid, Reliable Detection and Alarm
- Continuous, Unattended Operation
- Very Low False Alarm Rate
- Strategically Located Installation
- Automatic Shutdown of HVAC System
- Complete Building Coverage

"CW Sentry" Design Concept

- Solid-State SAW Vapor Sensor
- Simultaneous Detection of Nerve/Blister Agents
- Rapid and Reversible Detection
- Fully Automatic Operation and Reporting
- Compact, Durable, Low Maintenance
- Design for Fixed Installation Operation
- Compatible with Existing Fire Alarm Systems

"CW Sentry" Key Features

- Modular Design for Ease of Maintenance
- Built-in Air Pump
    - Adjustable
    - Sample 4 Locations up to 25 feet away
- On-Board Vapor Check Source
- Optional Remote Console Alarm Panel
- Self-Diagnosis to Detect Component Failure
- Interfaces with 24 VDC Fire Alarm Systems

Technical Approach to Implementation

- Assessment of Facility Chemical Vulnerability
  - External
  - Internal
- Survey of Building Engineering Facilities
  - Drawings (Air Ducts, Fans, Shutters, etc.)
  - Discuss with Bldg. Management and Engineers
- Select Location for Installation
- Install and Test CW Sentry
- Train Operations and Security Personnel

National Defense Industrial Association

14th Annual Security Technology
Symposium and Exhibition

Williamsburg, Virginia
June 15-18, 1998

Economic Espionage Act of 1996:
The Implications for Technology Transfer

Giovanna M. Cinelli, Esquire
Reed Smith Shaw & McClay LLP
8251 Greensboro Drive
McLean, Virginia 22102

ECONOMIC ESPIONAGE

- What is it?
  - ✦ industrial espionage versus aggressive competition
  - ✦ domestic versus international
- Legal responses?
  - ✦ theft statutes
  - ✦ intellectual property laws
  - ✦ Economic Espionage Act of 1996

STATISTICS

- Estimated losses: over $2 billion (American Society for Industrial Security
- FBI/DOJ responses: over 600 active cases through 1998
  - ✦ over 57 nations have been trying to obtain advanced technologies from U.S. corporations
  - ✦ active efforts by France, Japan, and Israel
  - ✦ Example companies affected: IBM, 3M Corporation, Eastman Kodak, Recon Optical; Avery Dennison, Bristol Meyer Squibb, AT&T, Gillette

[redacted]

ECONOMIC ESPIONAGE ACT OF 1996
§ § 1831 - 1839

- Designed to extend criminal jurisdiction to foreign governments, agents, parties or representatives who participate in activities which violate § § 1831-1832

[redacted]

EEA ELEMENTS
§ 1831

- Knowing "theft"
- By "fraud, artifice or deception"
- Of "trade secrets"
- "Carried away" or transmitted in any form
- To benefit any "foreign government, foreign instrumentality or foreign agent"

[redacted]

EEA ELEMENTS
(cont'd)

- A person who knowingly "copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates or conveys"
- A "trade secret"
- Without authorization
- For the benefit of a foreign government, agent or instrumentality

[redacted]

EEA ELEMENTS (cont'd)

- Knowingly "receives, buys, or possesses"
- A "trade secret"
- "Knowing" it to have been "stolen or appropriated, obtained or converted without authorization"
- For the benefit of a foreign government, agent or instrumentality

[redacted]

EEA ELEMENTS
§ 1832

- "Whoever," with intent to convert a trade secret
- Theft, or without authorization, "takes, carries away, or conceals"
- By fraud, artifice or deception
- obtains such "trade secret" information

KEY DEFINITIONS

- Trade secret (§ 1839(3)):

  ✦ "all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing"

OTHER REQUIREMENTS

- Trade secret owners must take reasonable measures to keep trade secret confidential

- The information (trade secret) derives "independent economic value, actual or potential" from not being known or readily ascertainable through public means

[redacted]

EXTRATERRITORIALLY APPLIED

- Statute applies to conduct outside the U.S. committed by a U.S. citizen or permanent resident

OR

to conduct by an organization organized under the laws of the U.S.

OR

if any act in furtherance of the offense was committed in the U.S.

APPROACH TO UTILIZATION OF THE STATUTE

- Risk analysis
- Technology or information involved
- Individuals with access, or likely access, to trade secret information
- Publicity
- Confidential protection of information once in the court system

[redacted]

METHODS OF COLLECTION WHICH PLACE INDUSTRY ON NOTICE OF POTENTIAL INDUSTRIAL ESPIONAGE

- Unsolicited requests for information through:
  - ✦ telephone
  - ✦ e-mail
  - ✦ fax
  - ✦ visit
- Request for response to marketing surveys
- Increased "hits" to company's Internet bulletin board or home page
- Inappropriate conduct during site visits
  - ✦ questions not directly related to visit
  - ✦ unusual number of methods of recording visits -- cameras, tape recorders, paper, laptops, handheld record compilers, dictaphones
  - ✦ unusual number of requests to make telephone calls
  - ✦ unusual attire
  - ✦ unusual qualifications of people on tour

[redacted]

COLLECTION METHODS
(cont'd)

- Unsolicited requests by foreign persons to market services to research facilities, academic institutions or companies. Invitations by foreign parties for U.S. technical experts to visit foreign sites to share technical expertise; *i.e.*, tied to "employment opportunities," intellectual property collaboration
- International exhibits, shows, seminars or conventions
- Joint Ventures and other Collaborative Efforts:
  - ✦ extensive opportunity to exchange information
  - ✦ wary of lopsided exchanges
  - ✦ varying degrees of respect and enforcement of nondisclosure agreements
  - ✦ over-submission of information during joint venture or other collaborative efforts negotiations

AREAS OF FOREIGN INTEREST IN TECHNOLOGY
(U.S. Government Studies)

- Aeronautics systems
- Armaments and energetic materials
- Chemical and biological systems
- Directed and kinetic energy systems
- Electronics
- Ground systems
- Guidance, navigation, and vehicle control
- Information systems
- Information warfare
- Manufacturing and fabrication
- Marine systems
- Materials
- Nuclear systems
- Power systems
- Sensors and lasers
- Signature control
- Space systems
- Weapons effects and countermeasures

FOCUSED AREAS OF HEIGHTENED INTEREST
(DOE Perspective)

- Ceramics
- Cermets
- Refractories
- Advanced automotive propulsion
- Composite materials
- Nuclear radiation sources
- Safeguard methods for nuclear materials
- Superconductivity
- Uranium enrichment

PLUS

- Environmental sciences - terrestrial (1994)
- Biomedical sciences - basic studies (1995)

COMPANY EFFORTS TO LIMIT "TRADE SECRET" THEFT

- Due diligence on employee background
- Training/sensitization
- Certifications or acknowledgments in NDAs
- Limiting access to those who really need to

Economic Espionage Act of 1996

This law was signed by President Clinton on October 11, 1996, culminating a nearly two-year effort on the part of the FBI and U.S. industry professionals to understand the scope of and effectively deal with the foreign economic espionage problem affecting the USA. This law also addresses the theft of trade secrets where no foreign involvement is found. The FBI initiated the Economic Counterintelligence Program in late 1994 with a mission to collect information and engage in activities to detect and counteract foreign power sponsored or coordinated threats and activities directed against U.S. economic interests. This focused effort resulted in a dramatic increase in FBI investigations and a realization that existing legal remedies were insufficient to address the scope and nature of the economic espionage problem. The Economic Espionage Act of 1996 resolves many gaps and inadequacies in existing federal laws by specifically proscribing the various acts defined under economic espionage and addressing the national security aspects of this crime. Additionally, it provides for criminal forfeiture of proceeds obtained as the result of economic espionage, preserves confidentiality in any prosecution, and provides for extraterritorial jurisdiction.

Economic Espionage Provisions

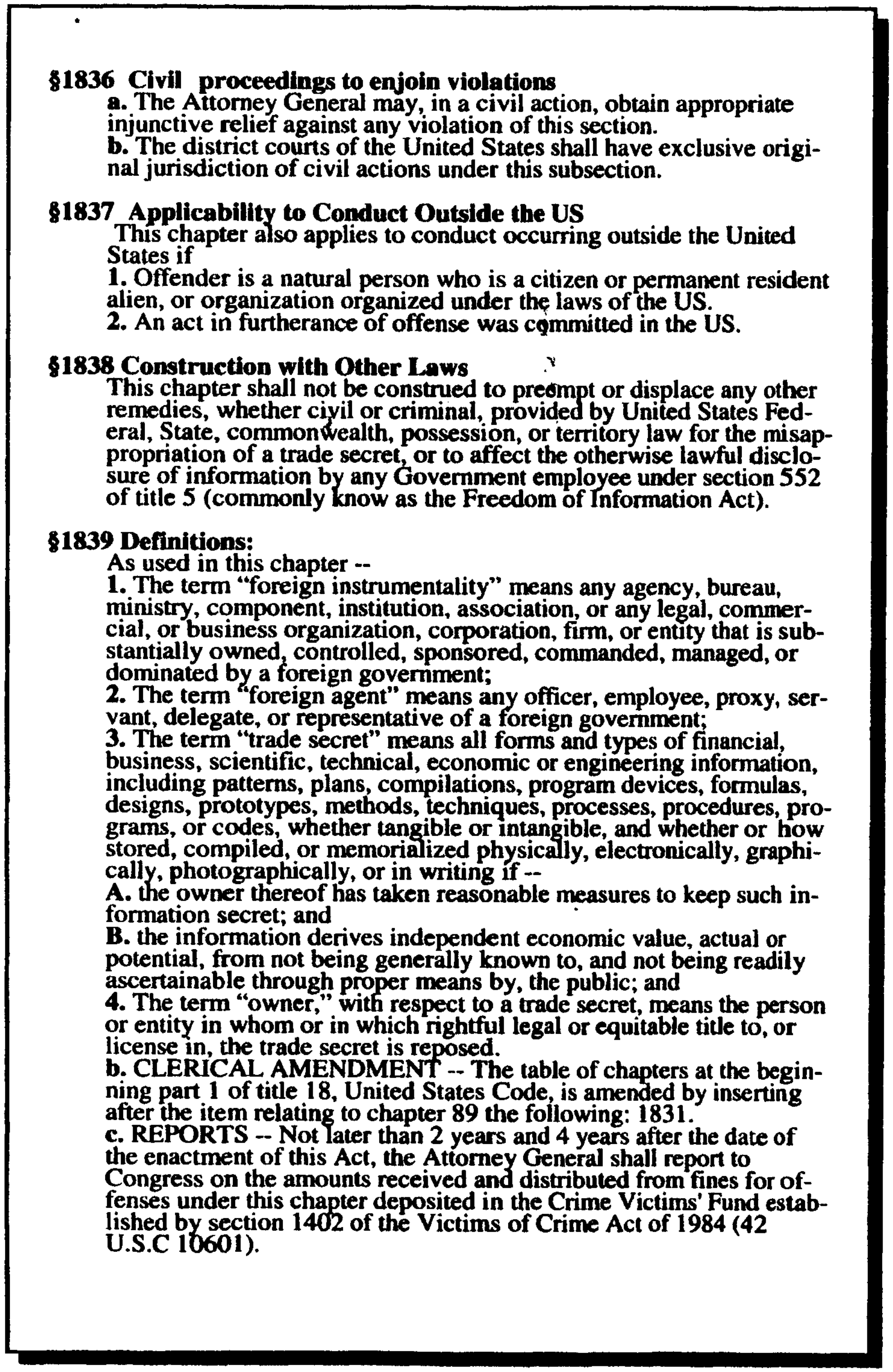
§1831 Economic Espionage [Agent of Foreign Power]
[Penalties: Persons: $500,000, 15 years; Organizations: $10,000,000]
a. IN GENERAL: Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly --
1. Steals, or without authorization appropriates, takes carries way or communicates, or by fraud, artifice, or deception obtain trade secrets;
2. Without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
3. Receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained or converted without authorization;
4. Attempts to commit any offense described in any of paragraphs 1 through 3; or
5. Conspires with one or more other persons to commit any offense described in any of paragraphs I through 4, and one or more of such persons do nay act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.
b. ORGANIZATIONS: Any organization that commits any offense described in subsection (a) shall be fined not more that $10,000,000.

§1832 Theft of Trade Secrets [Commercial Espionage]
[Penalties: Persons: $500,000, 10 years; Organizations: $5,000,000]
a. Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secrets knowingly --
1. Steals, or without authorizations appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtain such information;
2. Without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
3. Receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
4. Attempts to commit any offense described in paragraphs 1 through 3;
5. Conspires with one or more other persons to commit any offense described in paragraphs 1 through 3, and one or more such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.
b. Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

§1833 Exceptions [Law enforcement activity is exempt]
This chapter does not prohibit --
1. Any otherwise lawful activity conducted by a governmental entity of the United States, a State, or political subdivision of a State; or
2. The reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

§1834 Criminal Forfeiture [Additional penalty of forfeiture]
a. The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that the person forfeit to the United States;
1. Any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and
2. Any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violations, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.
b. Property subject of forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 8530), except for subsections d and j of such section. which shall not apply for forfeitures under this section.

§1835 Orders to Preserve Confidentiality
In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil procedures, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.



§1836 Civil proceedings to enjoin violations

a. The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.

b. The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.

§1837 Applicability to Conduct Outside the US

This chapter also applies to conduct occurring outside the United States if

1. Offender is a natural person who is a citizen or permanent resident alien, or organization organized under the laws of the US.

2. An act in furtherance of offense was committed in the US.

§1838 Construction with Other Laws

This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly know as the Freedom of Information Act).

§1839 Definitions:

As used in this chapter --

1. The term "foreign instrumentality" means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;

2. The term "foreign agent" means any officer, employee, proxy, servant, delegate, or representative of a foreign government;

3. The term "trade secret" means all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if --

A. the owner thereof has taken reasonable measures to keep such information secret; and

B. the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and

4. The term "owner," with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.

b. CLERICAL AMENDMENT -- The table of chapters at the beginning part 1 of title 18, United States Code, is amended by inserting after the item relating to chapter 89 the following: 1831.

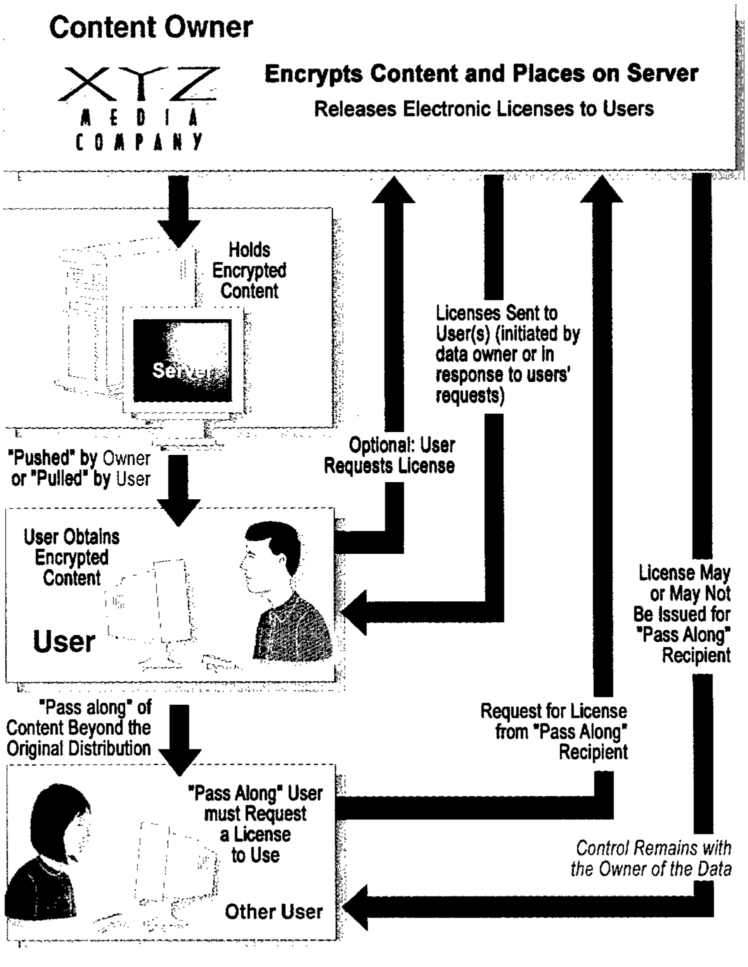
c. REPORTS -- Not later than 2 years and 4 years after the date of the enactment of this Act, the Attorney General shall report to Congress on the amounts received and distributed from fines for offenses under this chapter deposited in the Crime Victims' Fund established by section 1402 of the Victims of Crime Act of 1984 (42 U.S.C 10601).

Persistent Access Control or *How to Retain Control of Your Data After Delivery*

Today we can deliver information to users while safeguarding its confidentiality, ensuring its authenticity, and validating its origin. However, once information has been delivered, the originator must rely on the trusted behavior of the end user. Each user represents a vulnerability where copying or redistribution can occur. To protect information, we must forego many opportunities to use it. MRJ's technology breakthrough allows an originator to maintain control of information even after it has been delivered. In fact, the solution described here allows information to be posted and openly distributed (in encrypted form), allowing access only to authorized users and only as defined by the originator.

The three components of this invention[1] are:

- originator-*encrypted* information (where the key is known only to the originator).
- *electronic licenses* that control who may access the information as well as the specific accesses that are permitted (e.g., read-only, printing, display resolution, copying, time and duration of access, etc.).
- *hardware access mechanism* that mediates all input/output (access) requests—allowing only those permitted by the electronic license. A PC augmented with the hardware access mechanism would be compatible with current software and files. A tamper-detecting capability denies physical access to the hardware mechanism or to cryptographic variables.


Content Owner
XYZ MEDIA COMPANY
Encrypts Content and Places on Server
Releases Electronic Licenses to Users
Holds Encrypted Content
Server
Licenses Sent to User(s) (initiated by data owner or in response to users' requests)
"Pushed" by Owner or "Pulled" by User
Optional: User Requests License
User Obtains Encrypted Content
User
License May or May Not Be Issued for "Pass Along" Recipient
"Pass along" of Content Beyond the Original Distribution
Request for License from "Pass Along" Recipient
"Pass Along" User must Request a License to Use
Control Remains with the Owner of the Data
Other User

Some of the major benefits provided by this technology are described below. Pass through or secondary distribution remains under control of the originator. This means that a report *cannot* be copied, printed, or retransmitted beyond the individuals or offices on the original distribution list. Further, an originator can control access to products based on the originator's data. Any recipient of such a product may be required to obtain an electronic license from the owner of the original. Controlling the user's ability to copy, print, or retransmit sharply reduces the opportunity for leaks or redistribution.

Distribution logistics are dramatically improved. A file can contain items at multiple classifications and in different compartments. Images might be available at different resolutions or in different geographical areas. Users will be able to access only those parts which their license allows. Isolation is guaranteed because a user receives keys only to those compartments (or resolutions or areas) for which he or she has access approval. Software execution can also be controlled. In the electronic license, the software originator can specify the specific features available to each user or class of users.

Because the system operates with standard PC hardware and software and any media (e.g., CD-ROM, DVD), it will not stagnate, but will continue to benefit from and evolve with advances in the underlying technology of the PC.

MRJ Technology Solutions

Paul B. Schneck (703) 277-1618
schneck@mrj.com

[1] Based on technology developed at the MITRE Corporation by Paul B. Schneck with Marshall Abrams.

Counter-Competitor Intelligence: Applying the DOD Model to the Commercial Sector©

Session: Technical and Policy Focus Groups

Howard B. Low
Aegis Research Corporation
Space Engineering Center
1551 Vapor Trail
Colorado Springs, CO 80916
(719) 570-7041/567-9946
Fax (719) 570-7689/567-9898
E-mail: lowhowab@fafb.af.mil, hblow@pcisys.net

Counter-Competitor Intelligence:
Applying the DOD Model to the Commercial Sector ©

Good Morning. I am Bruce Low from Aegis Research Corporation. My topic has to do with one of today's hottest items in the security arena – how to defend yourself against the well organized and pervasive competitor intelligence threat.

Competitor intelligence (CI) is becoming a well understood problem – it's even making headlines in the popular press. There's a growing general awareness that it can be the basis for coordinated attacks against a business on several fronts, generally focusing on reasonably mundane activities to discover proprietary confidences (such as new product release timing, key supplier identification, or hiring campaigns targeting your key personnel). However, it can also extend to much more hostile activities, like trying to buy trade secrets by suborning employees or supporting takeover attempts. The quantity and quality of sensitive information that can be collected to further these goals has only recently gotten the serious attention of a whole new generation of executives.

What's *not* well understood is how to defend against a competitor's intelligence attack. Designing and implementing a sound program may be difficult for a company wanting to protect itself after realizing how good competitor intelligence organizations can be.

In the past, unless you were in one of the few industries that maintained an active defense, protecting proprietary information was the purview of the corporate legal department, with minor support from the security division. The defense strategy focused almost entirely on threatening employees with dire legal consequences if they didn't adequately protect their company's secrets. That approach will no longer suffice.

Analyzing the changing environment and marketplace pressures and determining that you need to take action to protect yourself are the all-important first steps, but they are just the beginning. The follow-on problem comes in designing and implementing a fully integrated program that responds to your needs analysis and fits your specific requirements.

There's very little training available to upgrade the skills of the existing security staff or executive team. How is a company going to develop this modern defense-in-depth? Where will they find the expertise? What is the answer to this dilemma?

One solution is to recruit one of the few successful practitioners from one of the leading edge industries with effective counter-competitor intelligence programs. This can be a very expensive solution that will only pay dividends once that person creates his own infrastructure within the company to implement his program, which can take a large budget and one to two years.

Another way to gain rapid expertise at a more reasonable price, possibly in conjunction with a hiring and training campaign, is to outsource - hiring consultants to rapidly set up and maintain your program. We're probably not talking about the same company that provides your guard service, although they will play a support role in the final plan, as will Legal and Human Resources. The best qualified teams come from the small number of providers whose staffs have the necessary operations, legal, security and counterintelligence skills to address the full range of disciplines required to defeat an aggressive competitor intelligence program (one that may even extend into corporate espionage and dirty tricks). These companies usually have strong teams of former Federal Government experts who gained their experience in the most aggressive competitor intelligence environment ever known – the Cold War!

A fully integrated counter-competitor intelligence program may be time consuming and difficult to implement, but the concept is easy to explain. Today's talk will focus on just such a concept – taking advantage of the risk-management methodology used on one of the Air Force's space programs, combining that approach with classic commercial practices currently in use.

The basics of this program are described in the following five step process.

- ***What*** do I protect? This is the most important step in the entire methodology. It defines the extent of the program by identifying those pieces of information that are so critical to our customer that he is willing to invest in a counter-competitor intelligence program to protect them.

The entire process is driven by the results of this analysis. This information is derived by one of several means. The quickest start up comes about if the customer has already identified the key facts that make him successful (based on a good understanding of his industry and knowing what information he needs to withhold from his competitors to keep them from overtaking him). This information comes from years of experience and lots of lessons learned the hard way. The driving force is that the customer has probably lost money in the past - customers and market share, critical design data, etc. – because he didn't protect himself from his competitors.

Lacking this foreknowledge, it's possible to develop these facts by a rigorous examination of the customer's business in the context of it's specific industry, maybe even hiring a competitor-intelligence company to tell him about himself. For example, is the product generally undifferentiated except for selling price, making production cost control information very important? Is the product's performance superior to others because of a secret design? Is a proprietary formula for the product responsible to strong sales, etc.? Defining both the categories and details of this critical information drives all the steps that follow. We can then derive who might want to collect the information and when and where it can be collected.

Clearly defining what you decide to protect is also an important step in any future legal actions against insider theft of trade secrets or other acts of corporate espionage under older statutes, as well as the more recent *Economic Espionage Act of 1996*. These laws require that information that a company might want to protect be clearly identified to employees charged with its protection. It also puts ethical competitor intelligence collectors (as well as corporate spies) on notice when viewing a clearly marked trade secret or piece of proprietary information.

- ***Why*** do I protect specific pieces of information? This step is a criticality analysis.

We will adapt one of the two basic approaches of military weapons system criticality analysis as the basis for this step. That approach questions, "Can the enemy use this information to copy the weapon system?". In our commercial example, the general equivalent, "Can the information be used to copy my product/process/etc.?" has clear application. The second half of this basic question goes to the discovery of related information. The answer to these questions in the defense world are further analyzed to define *how critical* the information might be, and then assigning a classification of Top Secret, Secret, Confidential, and even Unclassified But

Sensitive, depending on the degree of damage that would occur if the information were compromised.

The corporate world could easily follow that model, even using the same notations, e.g., "XYZ Corporation TOP SECRET". In our example, we might end up protecting information about a product's engineering, design, materials, components, manufacturing processes, unit costs, and marketing strategies and release dates all at different levels of 'classification'. In fact, the legal team would be happy to have our proprietary information this well defined because it makes it easier to assign damages in actionable cases.

The second basic military question, "Can this information be used to defeat my weapon system?" has less clear application, but we still need to perform this analysis so that we know about our vulnerabilities. At the minimum, a competitor might use this information for negative advertising. Worst case, this information can support a 'dirty tricks' campaign (e.g., it could be disastrous if a competitor drives up the price of a component in critically short supply).

- ***Who*** do I protect my critical information from?

The commercial marketplace is very different from the national security environment. Almost all of the threat comes from traditional business analysts using publicly available information. The threat from corporate espionage and foreign government intelligence services cooperating with a competitor is comparatively small (although on the rise – more about that later). The *who* is therefore the overt competitor intelligence community, ranging from 1-man shops simply cruising the Internet, to the very large multinational companies using sophisticated research tools to acquire every shred of relevant information in the public domain, no matter how obscure the source.

This doesn't mean that government sponsored intelligence doesn't happen, and that the information is not passed to foreign corporate competitors! Unlike this country, certain nations do share intelligence with their industries, especially when that industry is partially or wholly owned by that foreign government! To quote the National CounterIntelligence Center's (NACIC) 1997 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, "the theft, misappropriation, wrongful receipt, transfer, and/or use of US trade secrets and other economic information, particularly by foreign governments and their agents or instrumentalities, poses a direct threat to the health and competitiveness of the US economy".

If your business has foreign competitors who fit this scenario and it is likely that a foreign government is going to attack your security program, you will require the assistance of the Federal government to defeat them. Our government may find out about the attack before you do (through classified intelligence sources and methods) and come to you to arrange for a joint commercial-government response. Or, you might suspect that you're under attack by a foreign intelligence service and go to the government to get expert help dealing with threat.

Defining which threat applies to you requires analysis of the specific marketplace and the forces at work driving the competitor intelligence/foreign intelligence service effort. A multinational client protecting information about a revolutionary product in a very competitive defense market segment having major repercussions on his competitors, as well as impacts on his own share price on the stock market, can expect to be attacked by the professional competitor intelligence collection community, the internal competitor intelligence departments of individual competitors, and probably foreign government intelligence services. To quote the NACIC report again, "A 1996 Defense Investigative Service summary of foreign contacts indicated that numerous foreign countries displayed some type of suspicious interest in one or more of the 18 technology categories listed in the Military Critical Technology List (MCTL), which is published by the Department of Defense. These major technology categories include:

- Aeronautics systems.
- Armaments and energetic materials.
- Chemical and biological systems.
- Directed and kinetic energy systems.
- Electronics.
- Ground systems.
- Guidance, navigation, and vehicle control.
- Information systems.
- Information warfare.
- Manufacturing and fabrication.
- Marine systems.
- Materials
- Nuclear systems.
- Power systems.
- Sensors and lasers.
- Signature control.
- Space systems.
- Weapons effects and countermeasures."

On the other hand, there are many cases where information requirements are simpler, and the collection threat might be limited to competitors trying to anticipate each others' local marketing campaigns. For example, how much do you think Earl Scheib® spends to find out about what Maaco® is up to, and who do you think they hire to do the work? Probably not too much, and what they *are* interested in can be collected fairly easily by legal and ethical means.

Finally, let's clear up any potential confusion between protecting proprietary information from competitors and hiding information that is required to be filed for some statutory purpose from U.S. government entities. We oppose using a counter-competitor intelligence program to achieve illegal ends.

- ***When*** and ***where*** do I protect my critical information? *Exposure analysis* is the next step.

Exposure analysis looks at the prioritized list of information that requires protection, focusing on the most important first, and determines when and where that information is susceptible to collection, either in its final form, or as uncollated bits and pieces. An example of the former might be a carefully controlled final report to the Board of Directors that summarizes very sensitive line item costs in a product line. Using our example, "uncollated bits and pieces" are then the extra copies of individual bills from suppliers that go into the dumpster outside the fence.

These analyses also includes the collection of second order facts that can be used to derive protected information through analysis of what the military calls *indicators.* A good example of this might be spectroradiometric analysis of legally collected airborne effluents to detect chemical by-products that help a competitor understand your manufacturing process. A simpler example might be the number of cars in your factory's parking lot during the 2nd and 3rd shifts to help determine production output.

- ***How*** do I protect this information? Here were consider the full range of *countermeasures* available to defeat an intelligence attack.

The actions you take to protect yourself, based on the cumulative results of the *what*, *who*, *when* and *where* analyses, will include a combination of manufacturing and operations, administrative, legal, financial and security activities. The specific mix of countermeasures is tailored for each problem.

For example, traditional DOD counterintelligence, operations and communications security (OPSEC and COMSEC), and physical security countermeasure are effective against illegal and unethical corporate espionage methods, computer penetration, and other specialized technical operations, extending to foreign government-sponsored communications intercept and human intelligence (HUMINT) operations. On the other hand, limiting the damaged caused by legal research by industry experts using sophisticated tools may require more creative responses so that the security program doesn't get in the way of the overriding business interests of the customer.

There are dozens of tools on the full menu of countermeasure options, and they must be integrated through a master plan. Some are relatively simple to put in place, but others require specialized training to plan and implement. All have to be monitored (once in place) and fine-tuned to insure that they remain effective.

The bottom line is to plan carefully to protect your secrets: a poorly designed and executed counter-competitor intelligence protection plan is not only a waste of money, the resulting false sense of security will significantly increase the risk of losing the information you most want to protect!

Remember... once compromised, secrets aren't!

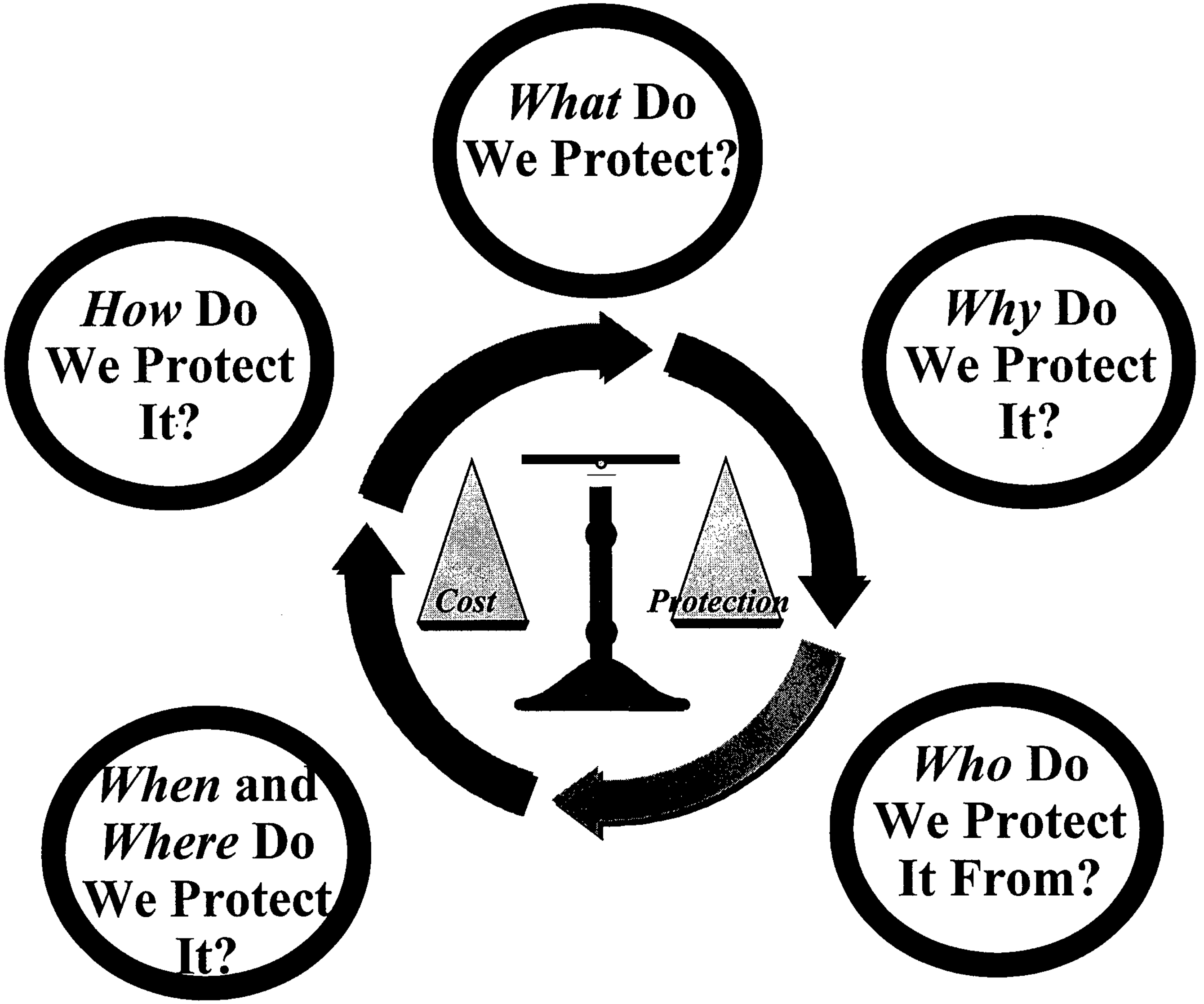
- END -

Aegis Research Corporation

©Howard B. Low 1998
Aegis Research Corporation, Space Engineering Center
1551 Vapor Trail, Colorado Springs, CO 80916
(719) 570-7041/567-9946 Fax (719) 570-7689/567-9898
E-mail: hblow@pcisys.net, lowhowab@fafb.af.mil

Counter-Competitor Intelligence:

Applying the DOD Model to the Commercial Sector©



What Do We Protect?

Why Do We Protect It?

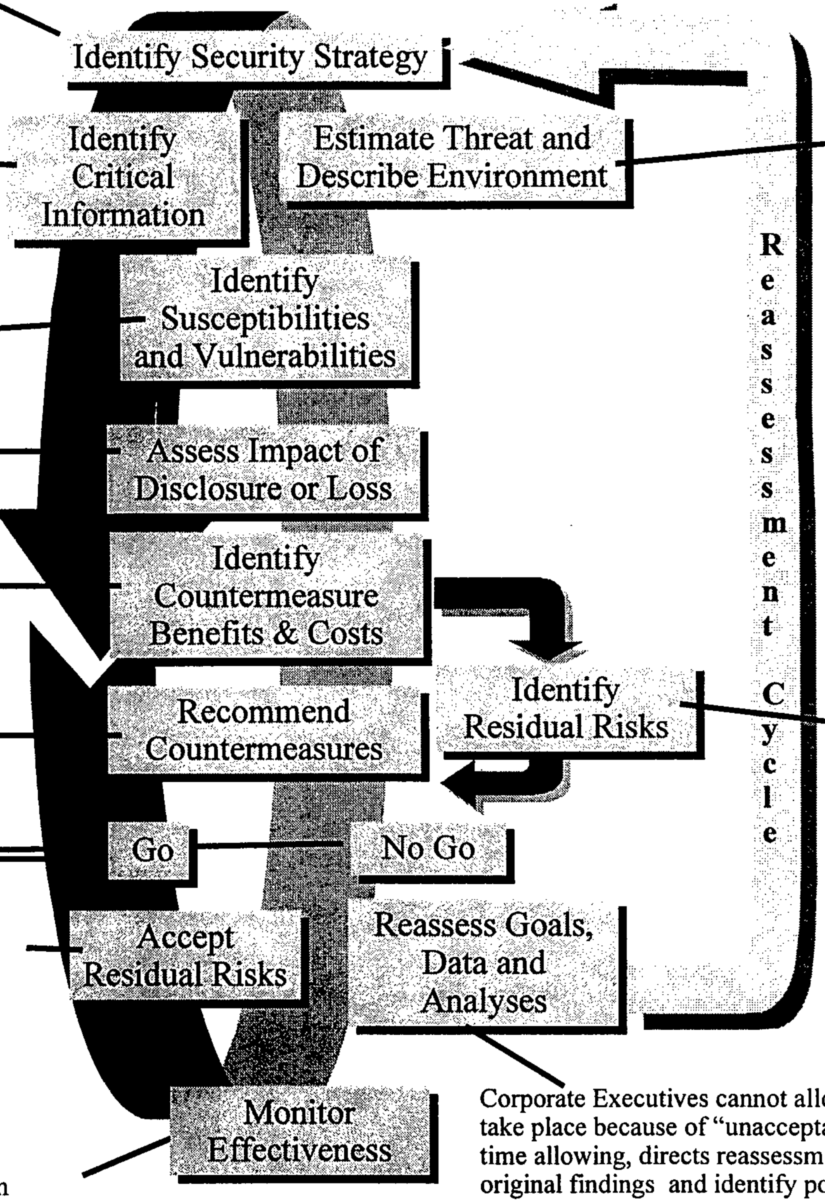
Who Do We Protect It From?

When and *Where* Do We Protect It?

How Do We Protect It?

©Howard B. Low 1998

Protection Planning Cycle



Corporate Executive Direction, Analyst Recommendation

Identify Security Strategy

What are the "secrets"?

Identify Critical Information

Estimate Threat and Describe Environment

What is the history of protection? Does anyone want to find out the "secrets" (now or in the future)? How are the secrets exposed to collection?

Could the "secrets" be collected? Does anyone have both the "capability" and the "intent" to collect them?

Identify Susceptibilities and Vulnerabilities

What damage will accrue if the secrets are discovered?

Assess Impact of Disclosure or Loss

Discuss potential active and passive CMs, the benefits and direct and indirect costs of each.

Identify Countermeasure Benefits & Costs

Identify Residual Risks

Describe the "left over" risks uncompensated by the mix of CMs.

Identify the "best" mix of CMs based on cost/benefit analyses.

Recommend Countermeasures

Reassessment Cycle

Corporate Executives make informed decision.

Go

No Go

Corporate Executives knowingly accept residual risks.

Accept Residual Risks

Reassess Goals, Data and Analyses

Corporate Executives cannot allow activity to take place because of "unacceptable" risks; time allowing, directs reassessment to validate original findings and identify possible alternatives.

Monitor Effectiveness

Assess CMs' effectiveness from intelligence or "mirror image" analyses; "fine tune" if required.

Program Protection Planning in the USAF TENCAP Program: A Real-World Application of Risk Management to Contain Security Costs©

Session: Technical and Policy Focus Groups

Howard B. Low
Aegis Research Corporation
Space Engineering Center
1551 Vapor Trail
Colorado Springs, CO 80916
(719) 570-7041/567-9946
Fax (719) 570-7689/567-9898
E-mail: lowhowab@fafb.af.mil, hblow@pcisys.net

Program Protection Planning in the USAF TENCAP Program: A Real-World Application of Risk Management to Contain Security Costs©

Good morning. I am Bruce Low, from Aegis Research Corporation.

My topic this morning is a review of how the Air Force Material Command's (AFMC) Space and Missile System Center (SMC) Space Applications Project Office (SAPO) acquisition security organization supports the USAF Tactical Exploitation of National Capabilities (TENCAP) program. I will be focusing on how we apply the principles of risk management to acquisition security in order to contain security costs.

Acquisition security underwent a major change in the early 1990's when the Department of Defense (DoD) moved from strict risk avoidance to tailored risk management as the basis for program protection planning and system security engineering. Program Executives no longer had to follow a set of inflexible guidelines that had little relationship to the threat; they could now actively manage their security programs based on specific threats.

Evolving methodologies and subroutines have allowed increasingly credible risk acceptance decisions as the security risk management approach has matured. Focusing on the highest threats while accepting residual risks translates into successfully targeting security investments to when and where they are the most effective.

The impact of this change on the Air Force has been far reaching, extending from major acquisition programs to smaller projects, like proofs of concept, technology demonstrations, and rapid prototyping. Today's talk focuses on the USAF TENCAP program as an excellent example of applying the security risk management approach to a family of smaller projects within individual TENCAP TALON programs.

Air Force Policy Directives and Instructions do not specify a methodology to achieve risk management goals, allowing senior Program Executives to choose government and industry 'best practices' to reach the desired program protection outcome within specific budget constraints. The SAPO, as the USAF TENCAP acquisition lead, chose a series of proven subroutines from other SMC programs to implement this DOD and USAF risk management direction.

These subroutines respond to these questions:

- *What must be protected?* The SAPO uses a standardized working aid (based on DOD, USAF and SMC classification guidelines for military space-related programs) to identify individual facts needing protection. These guidelines define what 'critical program information' (CPI) require protection as data that, if compromised, would significantly alter program direction; compromise program or system capabilities; shorten the expected combat-effective life of the system; or require additional research, development, test, and evaluation resources to counter the impact of CPI compromise. We look at the following areas:
  - Does the activity provide the U.S with a scientific, technical, operational, intelligence or battlefield advantage?
  - Is there reason to believe knowledge of the activity would allow a foreign nation to develop, improve or refine a similar item, or develop countermeasures?

- Does the activity provide information that would reduce or erode U.S. space dominance through denial of access to space in peace or war; reveal operational space doctrine; or, provide information on DOD reliance on civil or commercial space systems in crisis?

- *Why are the CPI protected?* We apply interim classification levels under Executive Order (E.O.) 12958 guidelines to protect CPI identified in the '*what*' step based on the information's criticality to either the U.S. or potential military and economic adversaries. Criticality analyses from the U.S. perspective address how the activity relates to mission requirements and capabilities; what opportunity does the activity provide to achieve technical or strategic surprise; what are the political impacts; and, what vulnerabilities are revealed? Criticality from an adversaries perspective addresses if the information allows them the opportunity to duplicate or counter the activity?

Depending on the responses to these questions, final classification levels assigned by an Original Classification Authority, as defined by the E.O. are:

- Top Secret - information that, if compromised, could cause 'exceptionally grave damage'.
- Secret - information that, if compromised, could cause 'serious damage'.
- Confidential - information that, if compromised, could cause 'damage'.

Another set of data that does not fall under the E.O. for formal classification, but is protected by the Government under contract law, are the USAF TENCAP contractor teams' proprietary data and trade secrets. Maintaining the privacy of this data, focusing on commercial information and products with particular interest in dual-use technologies, is essential to maintaining the health and competitiveness of this team.

- *Who is the CPI protected from?* The DoD assigns responsibilities for threat analysis support to individual national and military department security, intelligence, and counterintelligence (CI) activities. The resulting studies are published at varying levels of detail and classification, such as the unclassified National CounterIntelligence Center's *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage,* supplemented by classified notes. This report has recently reaffirmed that at least 23 countries continue both commercially sponsored and foreign intelligence service intelligence collection against government and commercial targets in the U.S.

The USAF TENCAP risk management team refines this general threat to the nation's secrets and tailors our security countermeasures to defeat collection activities of specific threats against USAF TENCAP activities and sites. This tailored threat response, provided by the implementing command, is detailed in the Program Protection Plan (PPP), which then steps through the remainder of the methodology to identify security costs, related benefits and residual risks. The USAF TENCAP Director has this information available as he makes decisions about security and CI countermeasures used to defeat specific threats to his projects. This is exactly the type of cost containment outcome envisioned by using a focused threat for the risk management process.

Program protection analyses are separate from *system* security engineering analyses reported in the System Security Management Plan (SSMP). The program protection analysis describe security activities supporting the total development environment. The SSMP looks at threats to each system, assessing what an adversary might be able to do to defeat or interfere with our system.

An example of one of the savings we have been able to affect in USAF TENCAP projects comes from avoiding duplication in developing the threat baseline for computer systems by using the conclusions of the 'software risk assessment' developed for Certification and Accreditation (C&A) by the Designated Approval Authority (DAA) as the threat for the PPP and SSMP.

Many TENCAP projects have focused on enhancing the processing and delivery of data to the warfighter through automated information systems – hardware, firmware and software – using either commercial or government off-the-shelf (COTS/GOTS) products whenever possible. Current USAF rules for the development of computer systems, even if unclassified, requires that we perform a risk assessment concerning these systems. Because we operate within an TS/SCI environment, we focus on the remaining HUMINT threat of the possibility that malicious logic might have been inserted into the COTS/GOTS software that forms the baseline for many of these projects. We do this through a modified software risk assessment that reviews the development history of the software by providing an audit trail of the people involved, as well as a review of the security status of facilities and platforms used. Not only does this software risk assessment support risk acceptance decisions by the USAF TENCAP Program Executive for program protection planning and system security engineering, it is also a major part of the C&A package submitted to the DAA.

These classified programs are relatively easy to assess. Software programmers and integrators already have active security clearances (e.g., they are in a trusted relationship with the Government based on various background checks), and the work is performed in a secure environment (the developmental computer system is protected from unauthorized physical and electronic access). Even though not required, most unclassified programs use the same cleared individuals in the same secure facilities used for classified programs. (There are management advantages to the contractor, Lockheed Martin Missile Systems, and it simplifies the Government's risk assessment process.)

COTS/GOTS software packages bring their own history with them, as well. Even though the Government may not be able to get a complete development history, with known personnel and access risks, the fact that the software has been developed by a major supplier and/or has been running virus-free for a period of time (especially in a classified mode at another Government location), reduces the risks that the Government accepts as part of the Program.

In the best case the software has been developed by individuals holding Government clearances on a system that has both physical and software security controls. In this case, the decision is very straightforward.

In less clear situations, the developers may be unknown, may be employees of a foreign company, be foreign national employees of a U.S. company, or simply be U.S. citizens who do not hold a security clearance. Higher risk scenarios might also include employees with a history of some activity that qualifies them for their company's Employee Assistance Program. Also, the development platform may have been located in an uncontrolled area where anyone could have had access to it, had dial-up access, or been able to access it via an Internet connection.

In this example, all of this information, summarized and weighted for both the C&A DAA and USAF TENCAP Program Executive, allows reasoned risk acceptance decisions on multiple fronts using the same data, saving time and money.

- *When and where can the CPI be protected?* During this step we perform 'exposure analyses' for critical and sensitive data, describing the full range of candidate countermeasures that could reduce the threats to both the *program* and the *system*. The analyst puts himself into the position of a hostile force, knowing the entire range of intelligence sources and methods available to that planner, and studies where CPI might be collected. *Program* protection countermeasures to this collection, as recommended in the Program Protection Plan (PPP), will clearly be security oriented, including such things as production line controls to account for classified hardware, OPSEC during testing and evaluation, enhancements to facility security to control personnel access, etc. On the other hand, *system* countermeasures reported through the SSMP might respond to a wide variety of technical susceptibilities. These also include some that are purely security, such as RTIC/RTOC (Real Time Information into the Cockpit/Real Time Out of the Cockpit) software features that defeat spoofing and encryption to nullify hostile intercepts of sensitive data, but could also include such things as system design features to counter jamming, hardening against soft kill mechanisms, etc.

- *How can the CPI best be protected?* Working together, acquisition, security, intelligence, and CI organizations recommend security and operations risk management options for the CPI from the broad range of candidates. Within the USAF TENCAP world, threat exposure analyses have led to a small number of specific countermeasure recommendations supplementing the TS/SCI environment, most of them fairly straightforward. For example, in the AIS discussion we had earlier, the greatest 'exposure' occurred during software development when it was most likely that malicious logic might be inserted into the code. The response was limiting physical and electronic access to the code to individual programmers who are in a 'trusted relationship' with the Government. Another example is encrypting data transmissions that contain sensitive test results that can be overheard by hostile intercept.

We provide the AFTENCAP Program Executive our best estimate of the costs and benefits of each security risk management option. These 'costs' may be direct (dollars), or indirect (negative schedule impact, reduced operational capability, etc.). In each case the decision brief clearly identifies the residual risks assumed by the Program Executive as a result of these risk acceptance decisions.

Quality control during implementation is critical to the success of the process – poorly executed program protection and system security management plans are not only a waste of money, the resulting false sense of security will significantly increase the risk of losing the information you most want to protect. Contractor activities taking place at a contractor location are supervised under the DD254, Contract Security Classification Specification. Government activities taking place at Government locations are controlled and monitored by Government members of the project Integrated Product Team (IPT), or under specific project Memoranda or Agreement (MOA).

To insure that the analyses and recommendations forming the basis for the Program Executives' residual risk decisions remain valid in the face of evolving government-sponsored and commercial threats, the Program Security Manager monitors and fine tunes the countermeasures package during implementation. This requires good CI feedback, as well as the use of other data management tools measuring the exposure of sensitive information.

AFMC, through the SAPO, has proven that this security risk management methodology, used elsewhere on larger space programs, is equally valid for fast moving smaller tasks (like the TENCAP Program's TALON projects). We continue to refine the process, applying the lessons we've learned to improve efficiencies and provide continuing successful program protection and system security engineering in the face of declining budgets. As a result of our extensive experience with this set of subroutines, we believe that this methodology can be applied anywhere in the DoD. It works equally well on programs with widely varying budgets and schedules. With modifications to accomodate minor variances in departmental guidelines, it can satisfy requirements is other USG Departments. It can even be successfully applied in the commercial world. We invite you to consider it to address your future needs.

- END -

References

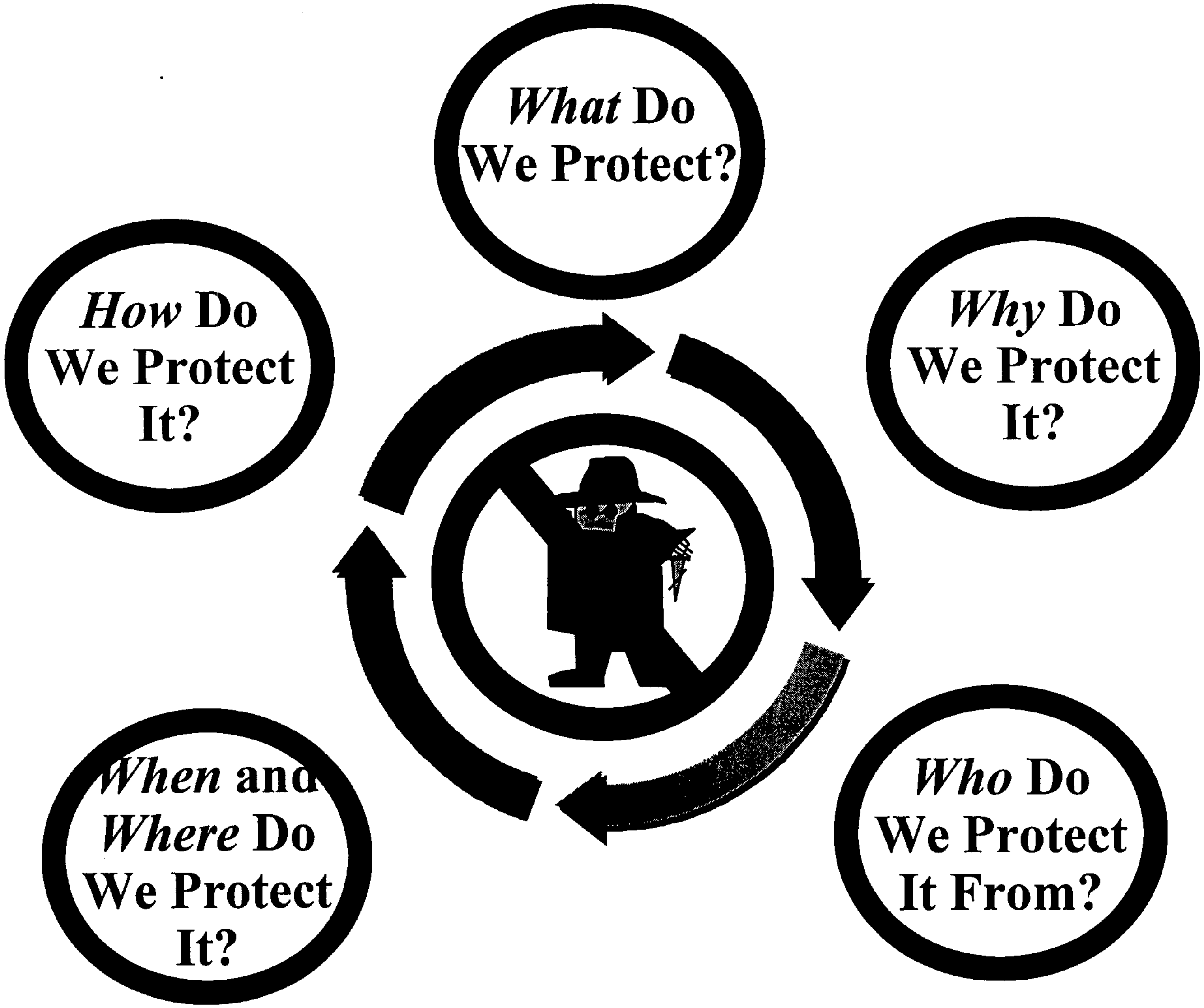
1. Economic Espionage Act of 1996, Title 18 U.S.C. 1831 et. seq.
2. Executive Order 12958, Classified National Security Information, 20 Apr 1995.
3. DoD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, (Includes Change 2), 06 Oct 1997.
4. DoD Directive 5200.39, Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection, 10 Sep 1997.
5. DOD 5200.1-M, Acquisition Systems Protection Program, 16 Mar 1994.
6. DoD 5200.1-R, DoD Information Security Program, Jan 1997.
7. Draft DOD Directive 3500.2, Space Systems Protect Program, 22 Aug 96.
8. ASPWG PH-1, Acquisition Systems Protection Program Workbook, Sep 1994
9. Air Force Policy Directive 31-7, Security, Acquisition Security, 02 Mar 1993.
10. AF Policy Directive 31- 4, Information Security, 01 Aug 1997
11. AF Instruction 31-401, Managing the Information Security Program, 22 Jul 1994
12. Air Force Instruction 31-701, Security, Program Protection Planning, 18 Feb 1994.
13. Air Force Instruction 31-702, Security, System Security Engineering, 18 Feb 1994.
14. Air Force TENCAP Program Management Directive, PMD TEN 1 (02)/PE#27247F, 13 Sep 95.
15. AF TENCAP Program Plan FY98, 01 Aug 1997.
16. Space Warfare Center AFTENCAP Project Process Handbook, Jun 1997.
17. Air Force Space Command/Space Warfare Center/Air Force TENCAP Transition Guide, (Draft) 01 Apr 1997.
18. Space Applications Project Office/Space Warfare Center, AFTENCAP Project Security Checklist, 30 Jan 1998.
19. Space Applications Project Office/Space Warfare Center, Project Plan Security Working Aid – 1, Project Protection Plan Outline, 30 Jan 1998.
20. Space Applications Project Office/Space Warfare Center, Project Plan Security Working Aid – 2, Data List, 30 Jan 1998.
21. Space Applications Project Office/Space Warfare Center, Project Plan Security Working Aid – 3, Project Security Strategy, 30 Jan 1998.
22. Space Applications Project Office/Space Warfare Center, Project Plan Security Working Aid – 4, Preliminary System Security Management Plan, 30 Jan 1998.
23. Space Applications Project Office/Space Warfare Center, Project Plan Security Working Aid – 5, Project Threat Survey, 30 Jan 1998.

Program Protection Planning in the USAF TENCAP Program

A Real-World Application of Risk Management to Contain Security Costs©

Aegis Research Corporation

©Howard B. Low 1998
Aegis Research Corporation, Space Engineering Center
1551 Vapor Trail, Colorado Springs, CO 80916
(719) 570-7041/567-9946 Fax (719) 570-7689/567-9898
E-mail: hblow@pcisys.net, lowhowab@fafb.af.mil



What Do We Protect?

Why Do We Protect It?

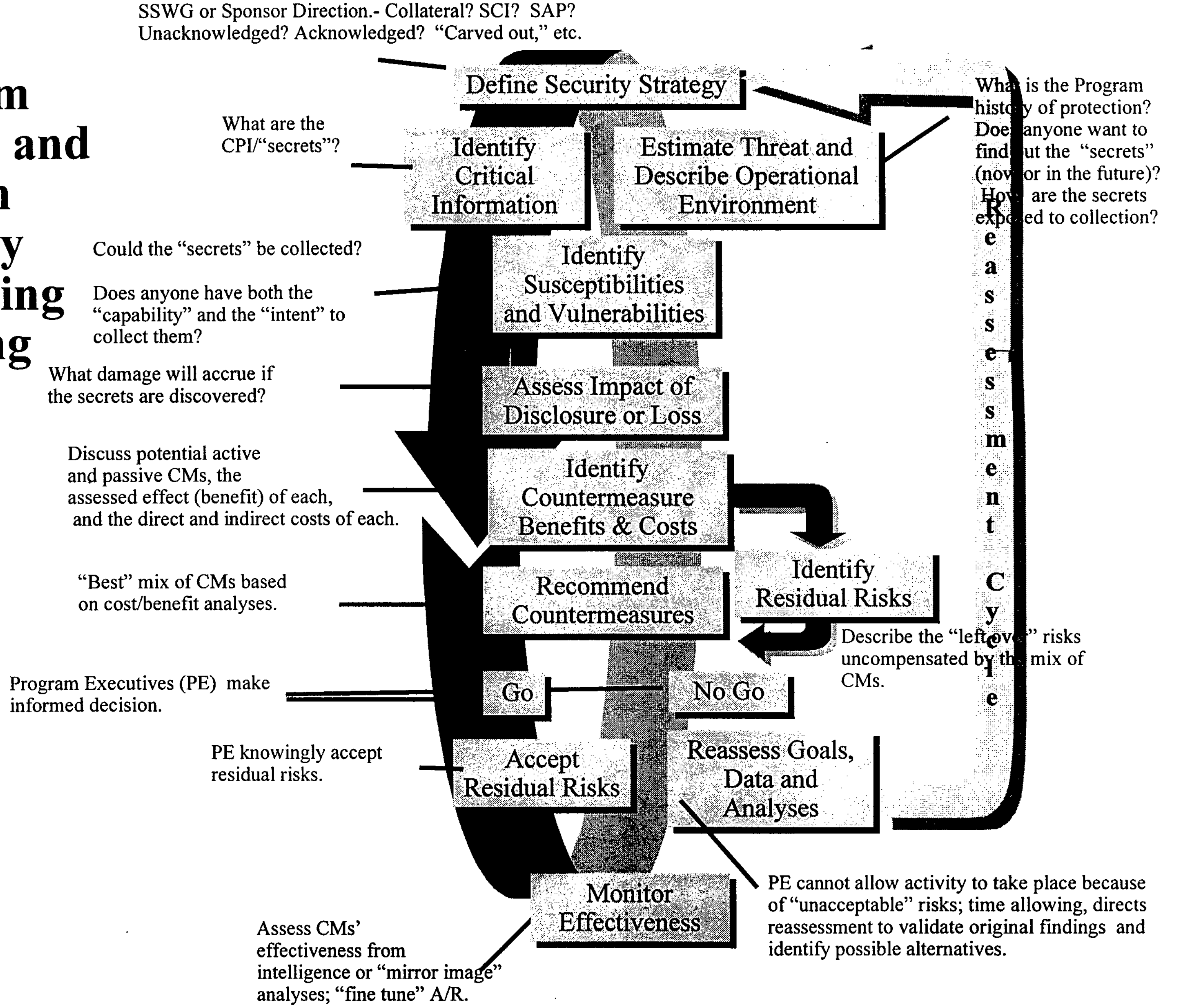
Who Do We Protect It From?

When and *Where* Do We Protect It?

How Do We Protect It?

©Howard B. Low 1998

Program Protection and System Security Engineering Planning Cycle



SSWG or Sponsor Direction.- Collateral? SCI? SAP? Unacknowledged? Acknowledged? “Carved out,” etc.

Define Security Strategy

What are the CPI/“secrets”?

Identify Critical Information

What is the Program history of protection? Does anyone want to find out the “secrets” (now or in the future)? How are the secrets exposed to collection?

Estimate Threat and Describe Operational Environment

Could the “secrets” be collected?

Does anyone have both the “capability” and the “intent” to collect them?

Identify Susceptibilities and Vulnerabilities

What damage will accrue if the secrets are discovered?

Assess Impact of Disclosure or Loss

Discuss potential active and passive CMs, the assessed effect (benefit) of each, and the direct and indirect costs of each.

Identify Countermeasure Benefits & Costs

Identify Residual Risks

Describe the “left-over” risks uncompensated by the mix of CMs.

“Best” mix of CMs based on cost/benefit analyses.

Recommend Countermeasures

Program Executives (PE) make informed decision.

Go

No Go

PE knowingly accept residual risks.

Accept Residual Risks

Reassess Goals, Data and Analyses

Reassessment Cycle

PE cannot allow activity to take place because of “unacceptable” risks; time allowing, directs reassessment to validate original findings and identify possible alternatives.

Monitor Effectiveness

Assess CMs’ effectiveness from intelligence or “mirror image” analyses; “fine tune” A/R.

Development of Security Engineering Curricula at US Universities

Session IV: Technology and Policy Focus Groups

Mary Lynn Garcia
Sandia National Laboratories
PO Box 5800 – 0762
Albuquerque, NM 87185-0762
(505)-844-2010
FAX: (505)-844-2193
mtgarci@sandia.gov

Development of Security Engineering Curricula at US Universities

Abstract

The Southwest Surety Institute was formed in June, 1996 by Arizona State University (ASU), New Mexico Institute of Mining and Technology (NM Tech), New Mexico State University (NMSU), and Sandia National Laboratories (SNL) to provide new educational programs in Security Engineering. This is the first science-based program of its kind in the United States, directed at educating Security Engineers to help government and industry address their security needs. Current courses include security system design, evaluation, principles and technology, the criminal justice system, and explosives surety.

Each member brings a unique educational capability to the Institute. NMSU provides a Security Technology minor, merging programs in Criminal Justice and Engineering Technology. NM Tech has a formidable explosives testing and evaluation facility. ASU is developing a Masters program in Security Engineering at their School of Technology located on a new campus in Mesa, Arizona. The Sandia National Laboratories security system design and evaluation process forms the basis for the Security Engineering curricula. In an effort to leverage the special capabilities of each university, distance education will be used to share courses among Institute members and eventually with other sites across the country.

The Institute will also pursue research and development funding in the areas of physical security, information security, computer modeling and analysis, and counterterrorist technology. Individual Institute members are currently working with sponsors from government and industry in areas such as counterterrorism, microelectronics, banking, aviation, and sensor development.

Introduction

The protection of critical assets has always been an important and difficult task. With the emergence of new threats including weapons of mass destruction, domestic terrorism, narcotics trafficking, international crime, and information warfare (1), this task has attracted more attention in both government and industry. At the same time, a heightened awareness has developed among the US public about the risks associated with high visibility targets. The World Trade center, Oklahoma City, and the Atlanta Olympics bombing are tragic evidence of the increased susceptibility felt by American citizens. This increased exposure leads to the realization that these risks and their consequences must be mitigated in order to assure the safety of our citizens as much as possible. Every day we are reminded of our susceptibility to attack. These attacks may be physical, electronic, or financial.

As in any other discipline, security requires the understanding and application of standard principles and concepts in order to achieve effective and consistent solutions. Today, the security industry is very fragmented, with no entry barriers. There is no system of accepted methodologies, basic principles, standard tools and tests, or universally accepted definitions. While security consultants can offer useful and pertinent services to their private industry and government customers, their effectiveness can be diminished due to the lack of grounding in common principles or an understanding of systems concepts. In all other professional fields there are unifying principles, basic concepts, and accepted definitions - in physics, electrical engineering, criminal justice, accounting, and medicine. Yet, in a field where researchers estimate the total cost of crime to be $425 billion each year, including $45 billion in property losses; and a $65 billion private security industry (2), there are no such unifying principles. The security professional of the future will be required to have a good understanding of technology, legal issues, and business practices to effectively protect people, property and information. By establishing educational programs that teach the common approaches, principles, and definitions, our universities and colleges can help bring necessary order and structure to this vital area.

Recognition of this problem inspired the creation of the Southwest Surety Institute (SSI) in 1996. Founding members Arizona State University- East (ASUE), New Mexico Institute for Mining and Technology (NM Tech), New Mexico State University (NMSU) and Sandia National Laboratories (SNL) were joined by Louisiana State University (LSU) in January, 1998. Programs in security engineering technology have been established at each university to provide unique, science-based curricula to students.

The discipline of security engineering will incorporate principles of business, technology, and criminal justice to educate a new generation of security engineers and managers who will be better able to make decisions as to when and how to protect assets. This science will also clarify the differences between safety and security, thereby adding some additional precision to security practices. Briefly, safety systems are needed to protect people and assets from abnormal environments, such as fire, earthquake, or electrical faults. Security systems, on the other hand, are meant to protect people and assets from attack by malevolent individuals or groups.

Program descriptions

The various members of the SSI currently offer three programs. New Mexico State University, located in Las Cruces, NM has created a security technology minor through the merging of select courses from the Criminal Justice and Engineering Technology departments. Students from each department take basic courses offered by the other department and then finish out the minor by taking a capstone course in security technology, where students are taught a design methodology and approach and learn the proper application of security technologies to balanced security systems. NMSU is planning on adding additional courses and upgrading the minor to a supplemental major. Table 1 shows a brief summary of courses available to students enrolled in the minor at NMSU.

Minor requirements for all students:	
CJ 101	Introduction to Criminal Justice
CJ 412	Introduction to Security Technology and Loss Prevention
ET 407	Security Technology
Additional requirements for Criminal Justice students:	
ET 307	Principles of Technology I
ET 357	Principles of Technology II
	One elective in Criminal Justice
Additional requirements for Engineering Technology students:	
CJ	3 electives in Criminal Justice OR 2 electives in Criminal Justice AND
CHEM 540	Explosives Surety (distance education delivery from NM Tech)

Table 1 - New Mexico State University - Minor Program in Security Technology

Arizona State University - East is creating a Masters program in Security Engineering Technology that will begin in the fall of 1998 at their School of Technology, located on a new campus in Mesa, Arizona. The degree is open to graduates of appropriate programs in engineering and engineering technology, as well as graduates of traditional criminal justice programs who have an acceptable technical background. This includes graduates of the programs at schools belonging to the Southwest Surety Institute. The program is designed to be completed in three semesters and one summer. Students will begin the course of study in the fall, with a target graduation by the end of the following summer. The program will include nine courses and an applied project, resulting in a total of 32 semester credit hours. The details of the courses and program of study are shown in Table 2.

Fall Semester	**CH**	***Winter Session***	**CH**	***Spring Semester***	**CH**
MET 510 Res Meth in Eng Tech	3	SET 594 Applied Project	2	SET 500 Security Law/ Regulation	3
MET 540 Econ Anal of Engineering Systems	3			SET 540 Risk Analysis/ Decision Making	3
SET 560 Physical Security Sys I	3			SET 561 Physical Security SysII	3
SET 570 Instrmntn Systems	3			SET 580 Forensic Technology	3
Totals	*12*		*2*		*12*
Summer Session					
SET 581 Computer Fraud	3				
SET 594 Applied Project	3				
Total	*6*				
Program total	**32**				

Table 2- ASU Master's Program in Security Engineering Technology - Sample Curriculum

In addition to the program described above, there will be a need to provide a set of normalization courses for those interested and otherwise qualified baccalaureate degree students with backgrounds that are lacking the technical basis necessary for the proposed program of study. It is possible for a motivated and mature student to obtain this framework in two semesters, if the student has a reasonable background in science and mathematics, such as provided by a typical liberal arts education. The normalization sequence may be completed at any member institution of the Southwest Surety Institute. These normalization courses may be taken at the students' current university or at ASU. This structure will support the use of a starting class every Fall at ASU, with graduation from the program at the end of the following summer, assuming the student attends full time.

NM Tech and LSU have enhanced their existing resources and capabilities to develop a counterterrorism education program. NM Tech operates the Energetic Materials Research and Testing Center (EMRTC), which has counterterrorism research facilities and programs already in place. LSU trains approximately 15,000 first responders each year, through its Anti-Terrorist Training Assistance Program and Fire and Emergency Training Institute. The two universities have recently joined together to provide training to international law enforcement agencies, conducted cooperatively at both schools. The Academy for Counterterrorism Education (ACE) was developed in response to the growing threat of terrorist acts on US military forces and civilian populations. Terrorist bombings such as the Khobar Towers in Saudi Arabia and in Oklahoma City demonstrate this alarming threat. While the US is spending millions of dollars on counterterrorism and force protection technology, state and local first responders are unprepared to deal with large explosive devices and weapons of mass destruction. Federal, military, National Guard, state and local police, fire, medical, and other first responders need training to prevent, detect, and respond to terrorist attacks.

The goal of ACE is to provide first responders with counterterrorism training. ACE will conduct a series of short courses and seminars at NM Tech, LSU, and selected locations throughout the US. Planned courses of instruction include Emergency Response Managers and Commanders Seminar (3 days), Chem/Bio/Explosives Responder Trainers (5 days) and a Large Explosive Device Post-Blast Analysis Course (5 days). Other planned educational support activities include “take-home" training and specialized equipment packages, an on-line distance education resource center, and graduate assistance and internships to expand the domestic base of expertise. For current updates on ACE, visit their homepage at *www.emrtc.nmt.edu/ace/.*

Individually, both NM Tech and LSU are also developing programs incorporating security engineering curricula. NM Tech is implementing an option (minor) program that will include courses in shock physics, explosives chemistry, explosives engineering, and security technology. In addition, students enrolled in doctoral programs in science and engineering may add these courses to their program of study and increase their knowledge of security concepts. In support of the Southwest Surety Institute educational goals and to exploit the unique capabilities offered by NM Tech, Explosives Surety Chemical Engineering 489, is currently offered via distance learning to NMSU and SNL; the course is expected to be offered at ASU as part of the MS program.

LSU is planning on an initial offering of a one week course entitled Design and Evaluation Process for Physical Security Systems in July of 1998 and will develop additional courses to supplement this program over time. The one week course, taught by experts from Sandia National Laboratories, will be repeated twice each year in the New Orleans area as part of the LSU continuing education program. These offerings allow access to the education and training programs of the Institute for those interested in continuing professional education or refresher training, such as law enforcement or industrial security managers.

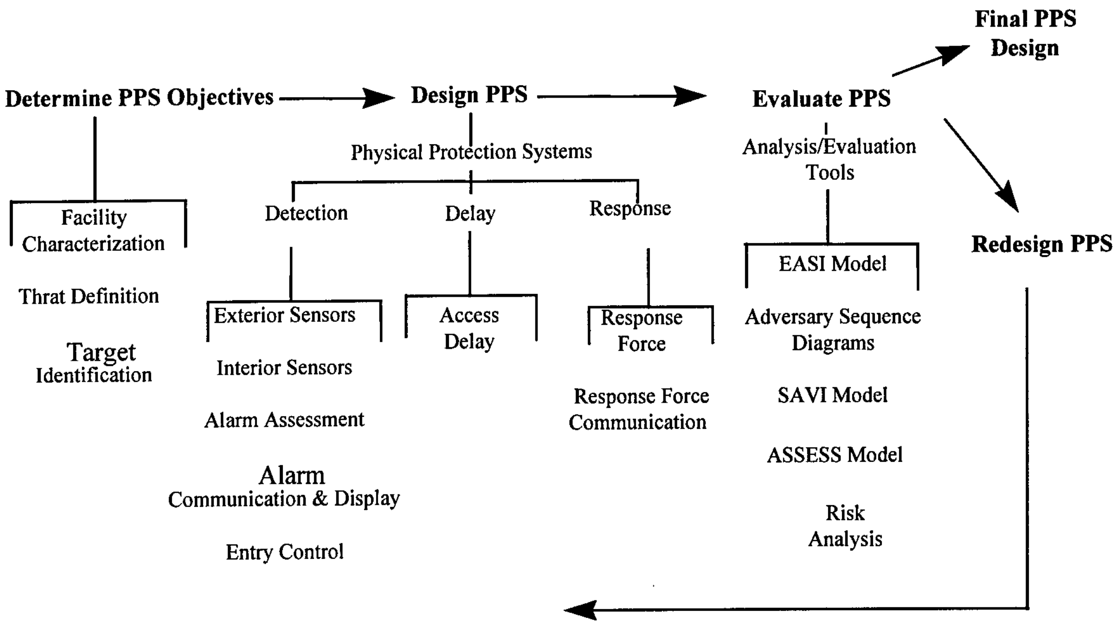


Fig. 1 – Sandia Design and Evaluation Process Outline

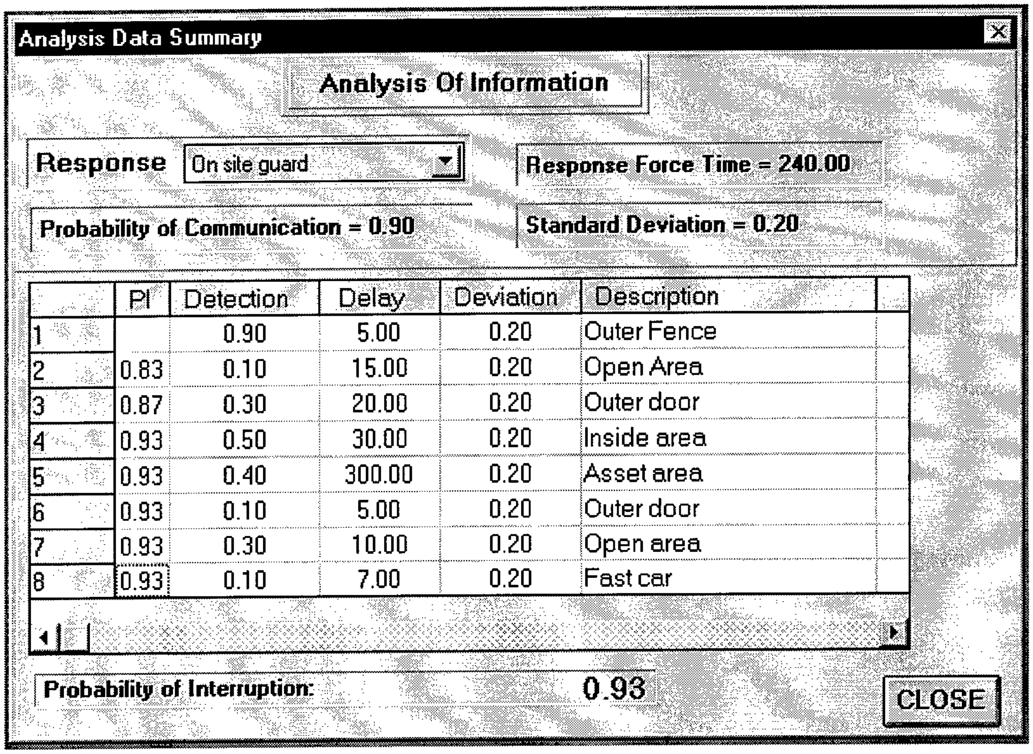
All of the programs will bring together engineering, business and criminal justice elements in order to create a new generation of security engineers and managers who will be better prepared to effectively achieve the security goals of their organizations. These programs are based on the design and evaluation methodology developed at SNL over the past 25 years. An outline of the approach is shown in Figure 1. This approach integrates people, procedures and equipment into a balanced and effective system that protects targets from the identified threat. The process is dependent on the use of performance measures, so that security professionals and their business managers will have a way of identifying what improvements they will achieve by performing proposed upgrades. A major benefit of these educational programs will be the capability of graduates to effectively use existing computer analysis models to predict the performance of a security system using such performance measures as probability of detection, delay times, response force times, probability of communication and assessment, and probability of interruption or neutralization.

In an effort to leverage the special capabilities of each university, distance education will be used to share courses among Institute members and eventually with other sites across the country. A grant of $2 million dollars from the US government will provide the initial funding required to establish the various programs.

Benefits/Future path

Perhaps the greatest need in the field of security today is in analysis of systems, i.e., predicting when enough has been done to meet the system objectives. This can be accomplished through the use of models already developed by the Department of Energy that incorporate performance measures as inputs and produce probabilities of success as the output. The unique aspect of these programs is centered on analyzing proposed security system designs or upgrades to help determine if the change is cost effective

An example of these analytic results is shown in Figure 2. If we assume that an intruder has entered a facility by climbing a fence, crossing an inner area, defeating a door, stealing the target, then exiting the facility, the result of a typical analysis can be seen. We can use the probability of interruption to predict whether the response force will arrive at the target or boundary in enough time to interrupt the adversary.



Response: On site guard

Response Force Time = 240.00

Probability of Communication = 0.90

Standard Deviation = 0.20

	PI	Detection	Delay	Deviation	Description
1		0.90	5.00	0.20	Outer Fence
2	0.83	0.10	15.00	0.20	Open Area
3	0.87	0.30	20.00	0.20	Outer door
4	0.93	0.50	30.00	0.20	Inside area
5	0.93	0.40	300.00	0.20	Asset area
6	0.93	0.10	5.00	0.20	Outer door
7	0.93	0.30	10.00	0.20	Open area
8	0.93	0.10	7.00	0.20	Fast car

Probability of Interruption: 0.93

Figure 2 - Adversary Path Analysis

Through the use of performance measures, graduates of these programs will have the knowledge to first determine the security objectives of the system, design the proper mix of detection, delay and response technologies to meet the objectives, and then analyze proposed additions or upgrades. This capability will lead to enhanced communication within the security community and reinforce efforts to provide useful and effective systems. The increase in system performance can then be used to make an informed decision, before the actual implementation of the system, as to the adequacy of the proposed changes. This will provide a rationale for any expenditure, as well as a measure of expected system performance, which can then be used to mitigate the risk of loss of the asset. Justification of the cost compared to improved performance will enable the enterprise to make good decisions on where to spend limited dollars.

As the programs grow and develop, existing tools and approaches will be modified and improved to create tools useful to all segments of the government and private industry, across the entire spectrum of protection requirements, from lowest to highest. These include development of new technologies to detect and assess causes of alarms, integration of technology into effective sub-systems, creation of new unclassified databases for use in computer models, and creation of new computer models to allow for validated predictions of security system performance. Applications in physical security, information security, computer modeling and analysis, and counterterrorist technology form the core of future research and development proposals by institute members.

This new generation of security professionals will posses the training and knowledge to test components, determine required performance measures, fit security objectives into the larger goals of the enterprise, provide information to management to help make investment decisions, and lessen risk to the enterprise by understanding the level of protection offered by the security system.

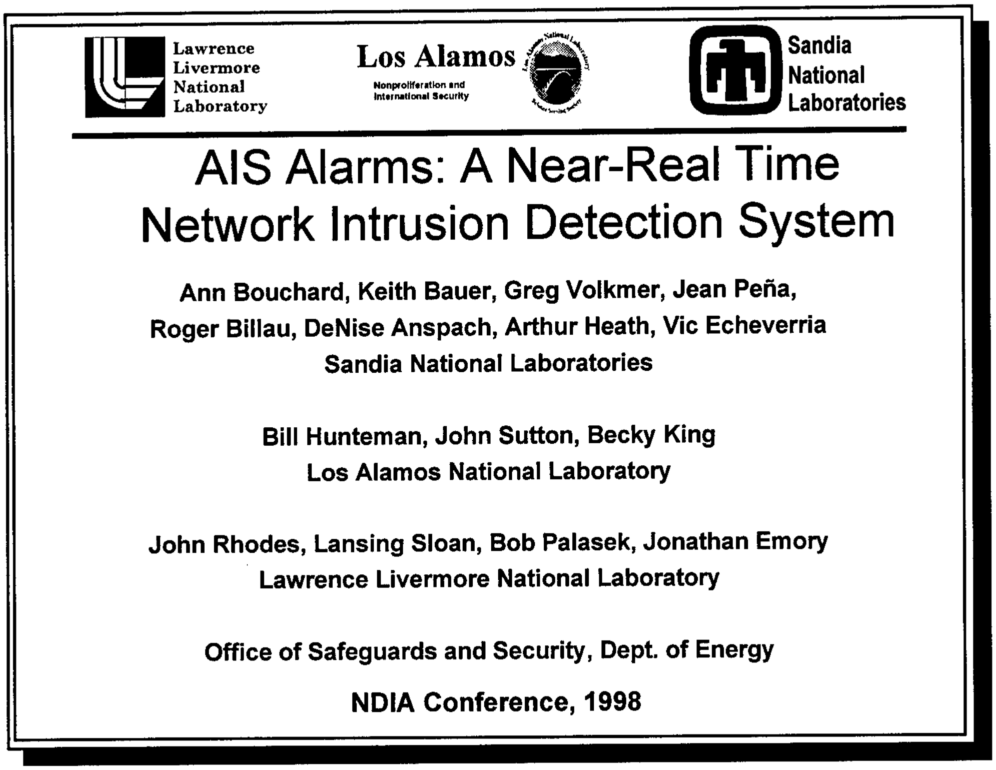
Summary

The Southwest Surety Institute was formed in 1996 to create unique, science-based educational programs in security engineering. The programs will integrate business, technology, and criminal justice elements to educate a new generation of security professionals. Graduates of the programs will better understand basic security system design and evaluation and contribute to strengthening of the body of knowledge in the area of security. A systematic approach incorporating people, procedures, and equipment will be taught that will emphasize basic security principles and establish the science of security engineering. The use of performance measures in the analysis of designed systems will enable effective decisions by an enterprise and provide the rationale for investment in security systems.

Along with educational programs, Institute members will conduct original research and development built on existing relationships with sponsors from government and industry in areas such as counterterrorism, microelectronics, banking, aviation, and sensor development. Additional information and updates on the Southwest Surety Institute are available via the Institute home page at *www.emrtc.nmt.edu/ssi.*

References:

1. "Summer blockbuster: Assessing the real threat," Boston Globe, August 20, 1997
2. "The Economics of Crime," Business Week, December 13,1993, pp. 72-81



Lawrence Livermore National Laboratory | Los Alamos Nonproliferation and International Security | Sandia National Laboratories

AIS Alarms: A Near-Real Time Network Intrusion Detection System

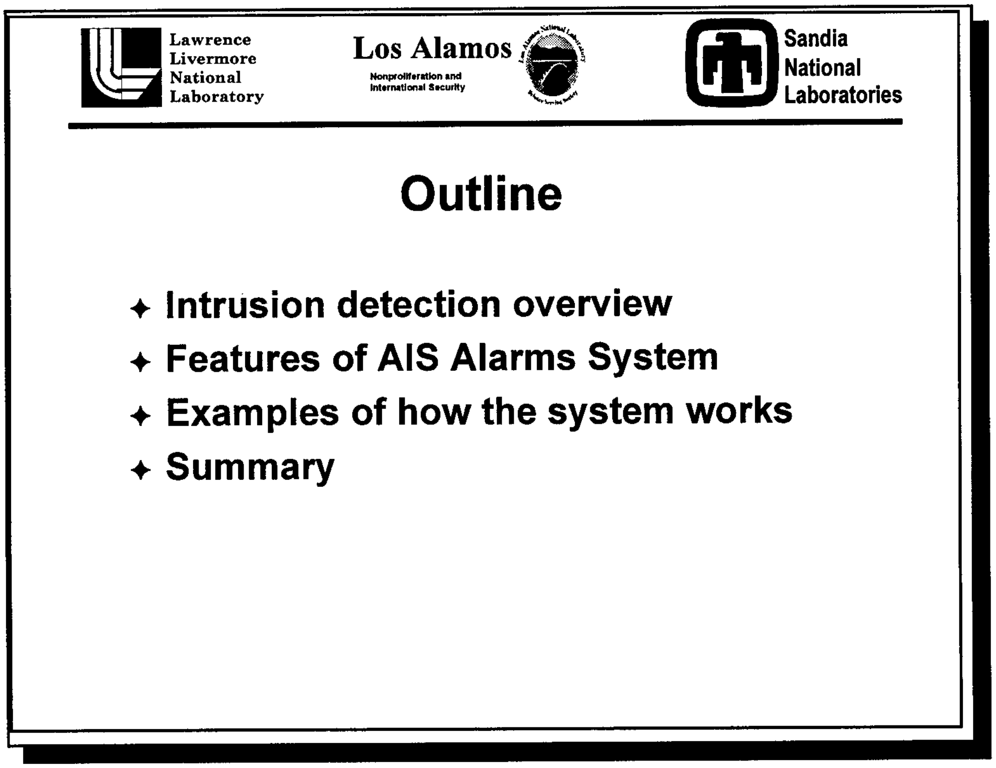
Ann Bouchard, Keith Bauer, Greg Volkmer, Jean Peña,
Roger Billau, DeNise Anspach, Arthur Heath, Vic Echeverria
Sandia National Laboratories

Bill Hunteman, John Sutton, Becky King
Los Alamos National Laboratory

John Rhodes, Lansing Sloan, Bob Palasek, Jonathan Emory
Lawrence Livermore National Laboratory

Office of Safeguards and Security, Dept. of Energy

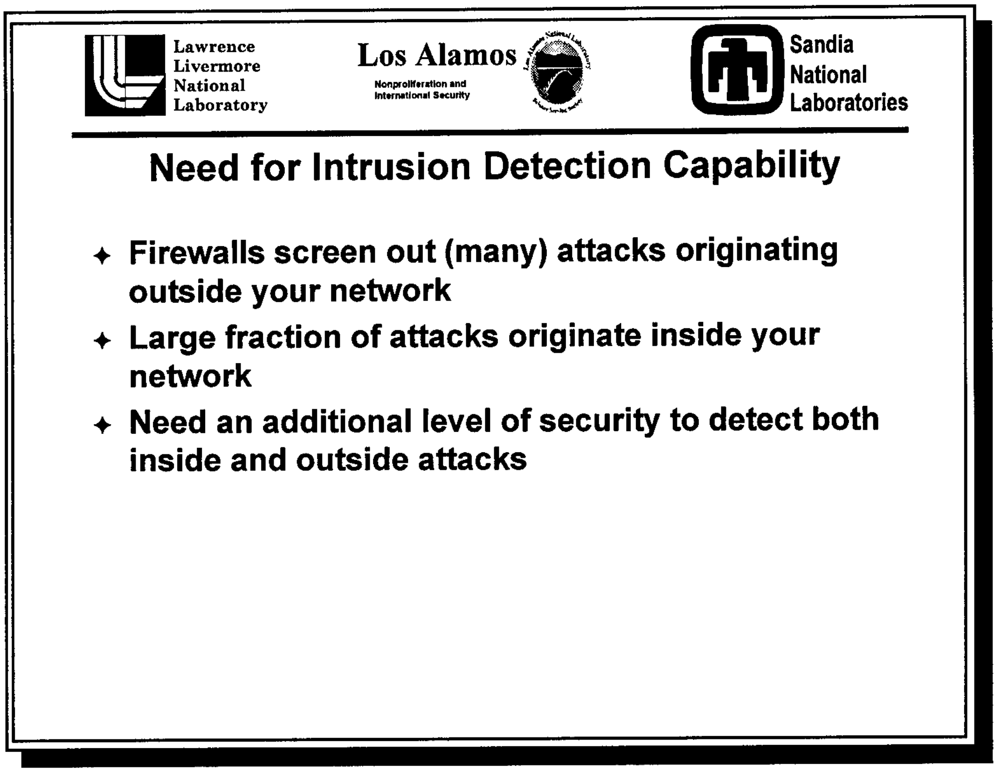
NDIA Conference, 1998



Lawrence Livermore National Laboratory | Los Alamos Nonproliferation and International Security | Sandia National Laboratories

Outline

- Intrusion detection overview
- Features of AIS Alarms System
- Examples of how the system works
- Summary



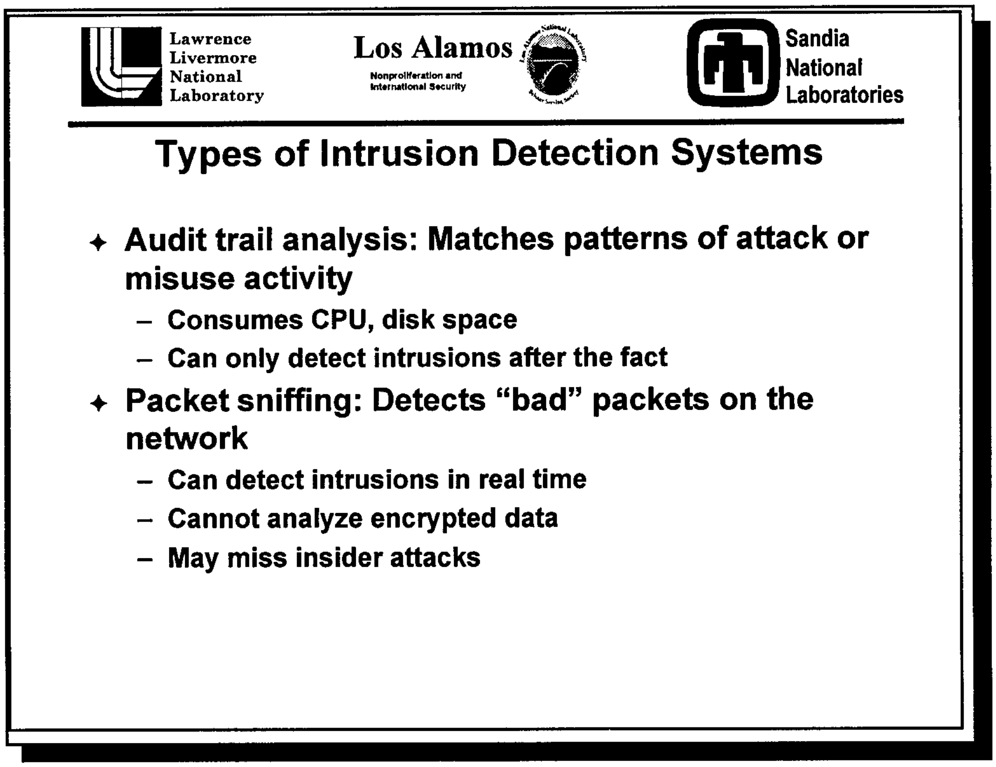
Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

Need for Intrusion Detection Capability

- Firewalls screen out (many) attacks originating outside your network
- Large fraction of attacks originate inside your network
- Need an additional level of security to detect both inside and outside attacks



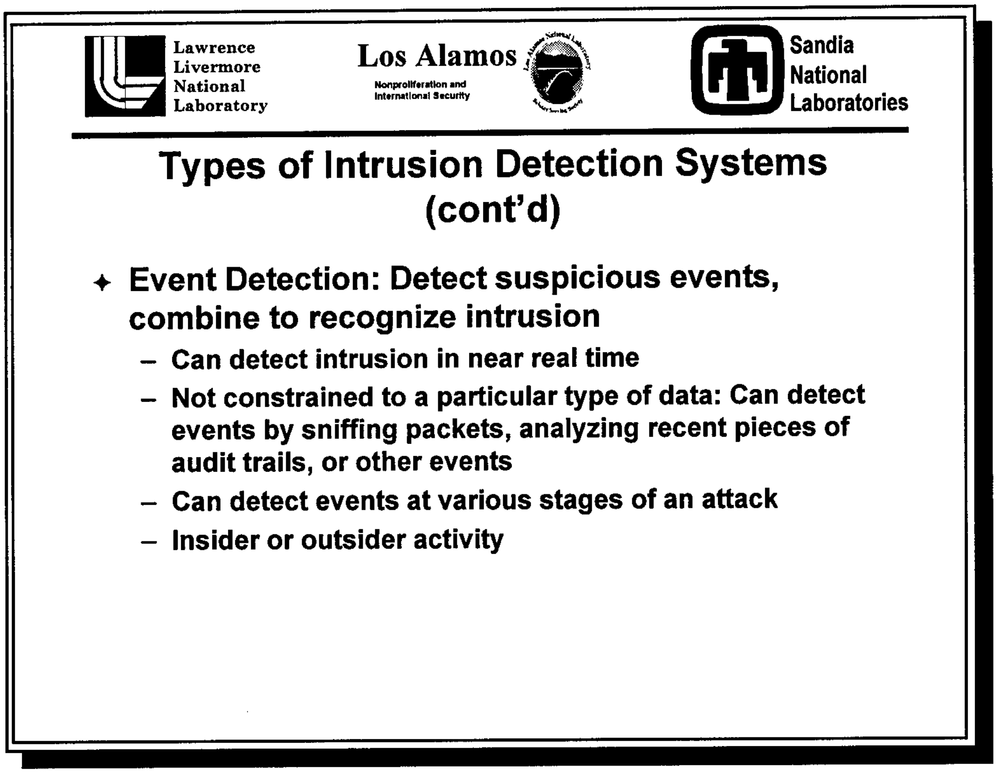
Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

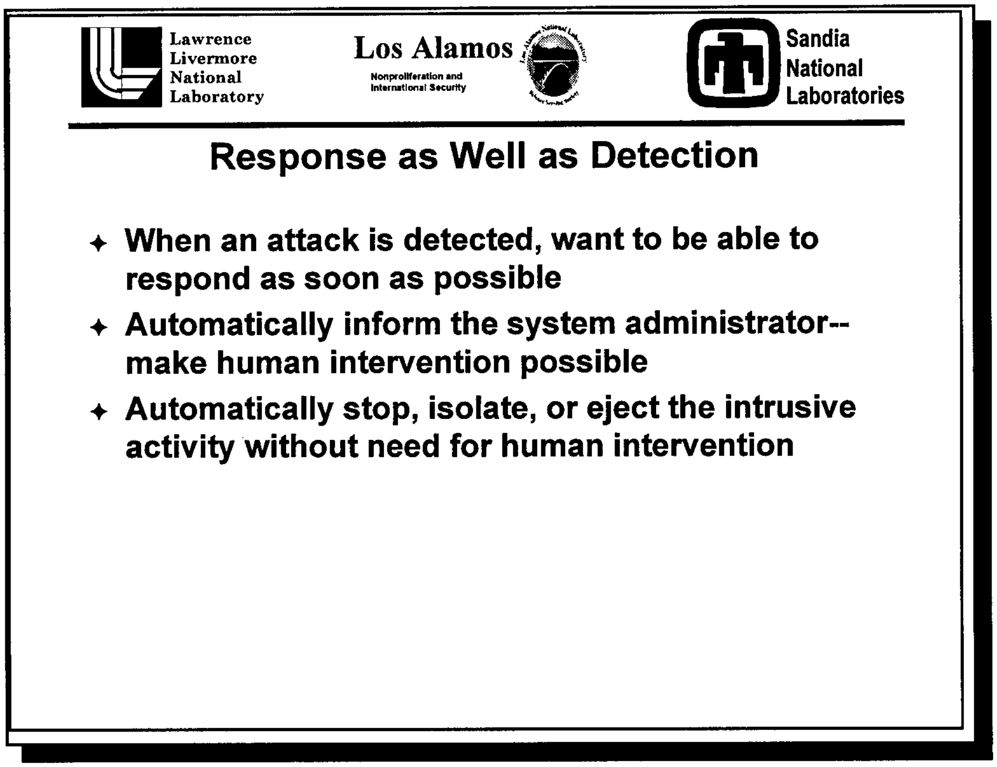
Types of Intrusion Detection Systems

- Audit trail analysis: Matches patterns of attack or misuse activity
  - Consumes CPU, disk space
  - Can only detect intrusions after the fact
- Packet sniffing: Detects "bad" packets on the network
  - Can detect intrusions in real time
  - Cannot analyze encrypted data
  - May miss insider attacks



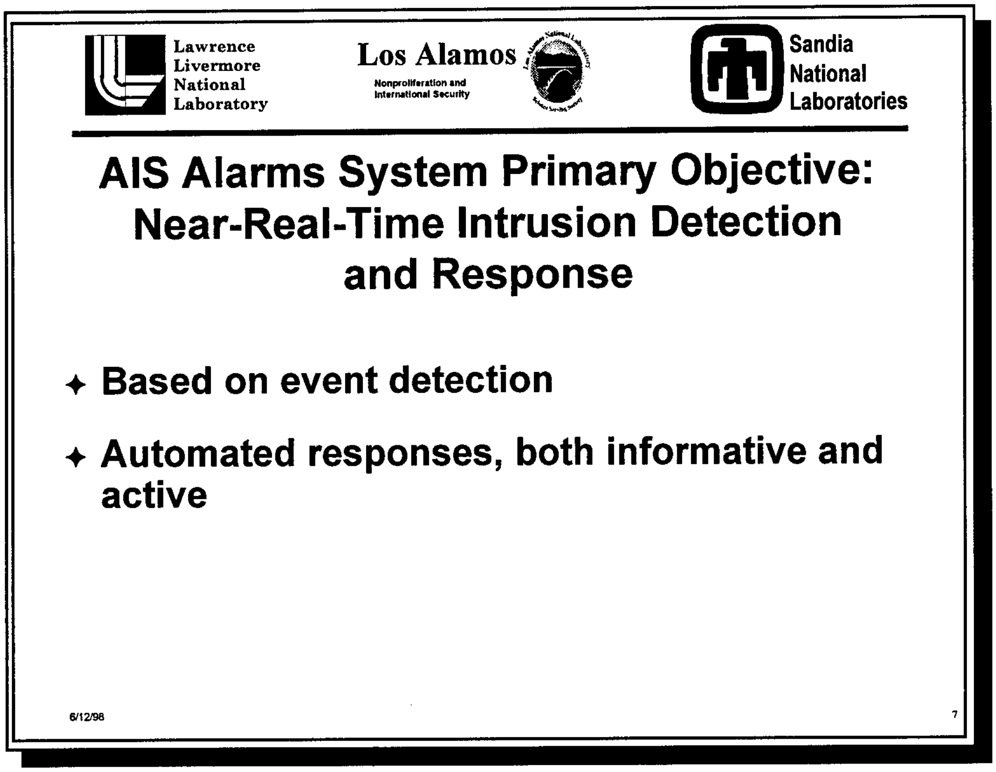
Types of Intrusion Detection Systems (cont'd)

- Event Detection: Detect suspicious events, combine to recognize intrusion
  - Can detect intrusion in near real time
  - Not constrained to a particular type of data: Can detect events by sniffing packets, analyzing recent pieces of audit trails, or other events
  - Can detect events at various stages of an attack
  - Insider or outsider activity



Response as Well as Detection

- When an attack is detected, want to be able to respond as soon as possible
- Automatically inform the system administrator--make human intervention possible
- Automatically stop, isolate, or eject the intrusive activity without need for human intervention



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

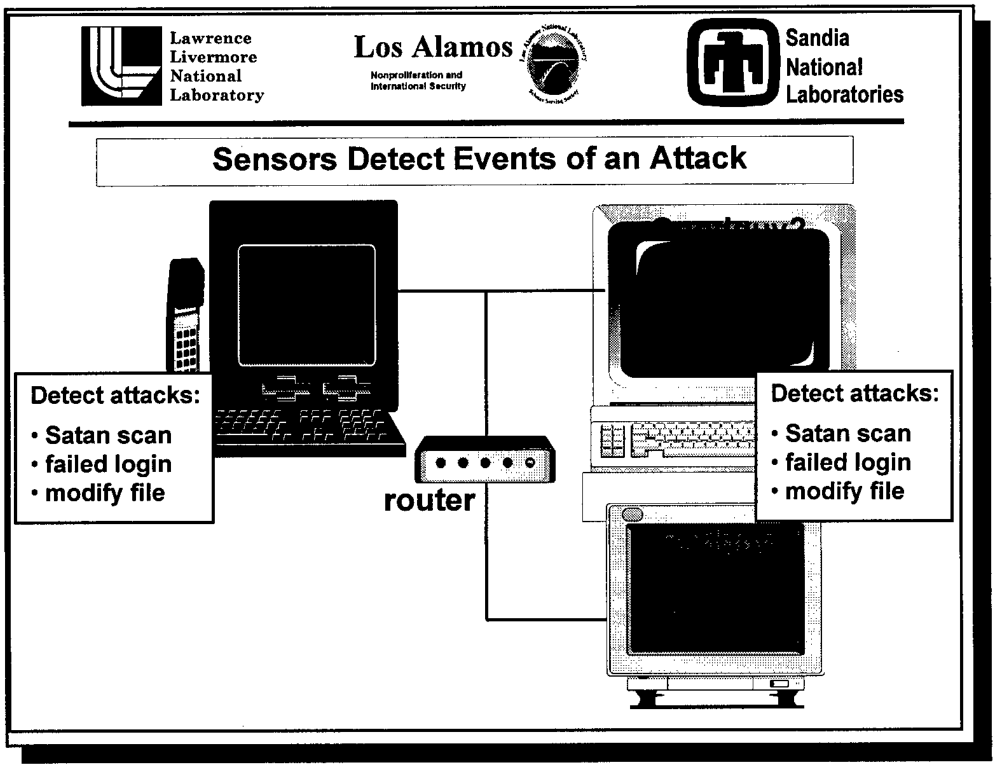
Sandia National Laboratories

AIS Alarms System Primary Objective: Near-Real-Time Intrusion Detection and Response

- ✦ Based on event detection
- ✦ Automated responses, both informative and active

6/12/98

7



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

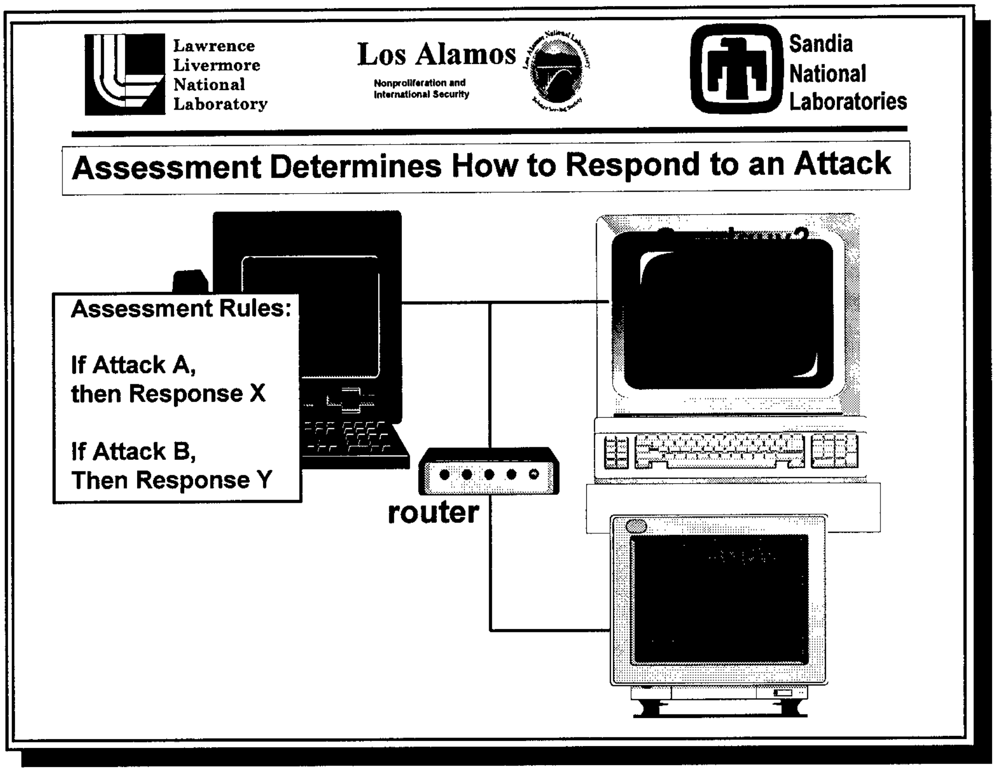
Sandia National Laboratories

Sensors Detect Events of an Attack

Detect attacks:
- Satan scan
- failed login
- modify file

router

Detect attacks:
- Satan scan
- failed login
- modify file



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

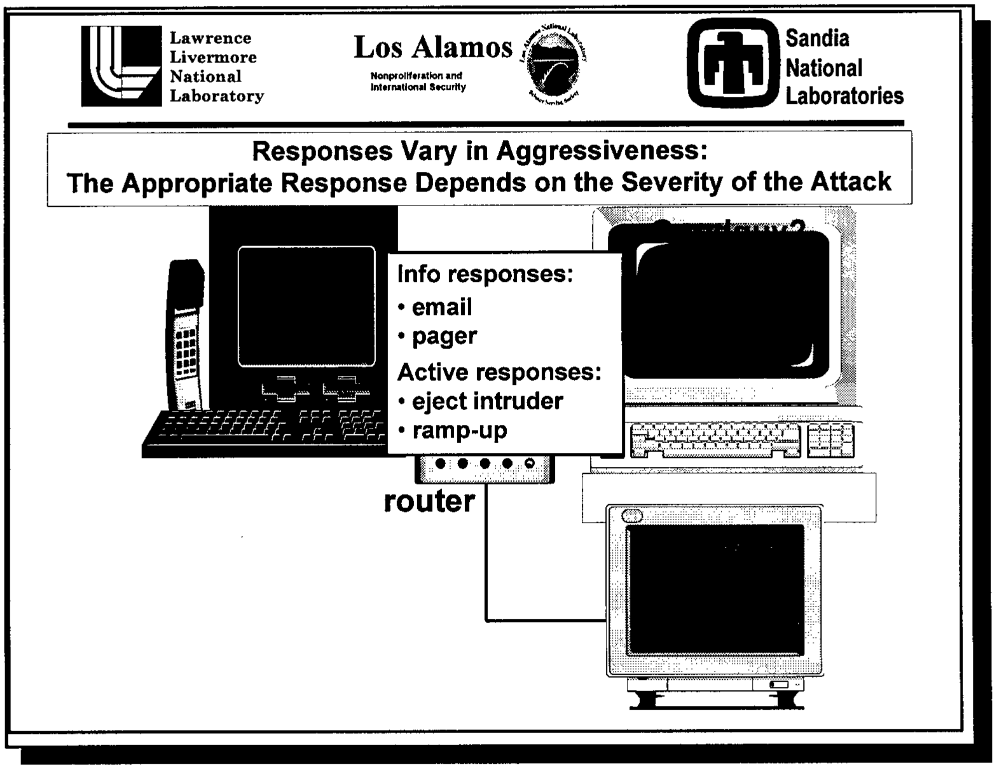
Sandia National Laboratories

Assessment Determines How to Respond to an Attack

Assessment Rules:

If Attack A,
then Response X

If Attack B,
Then Response Y



Lawrence Livermore National Laboratory

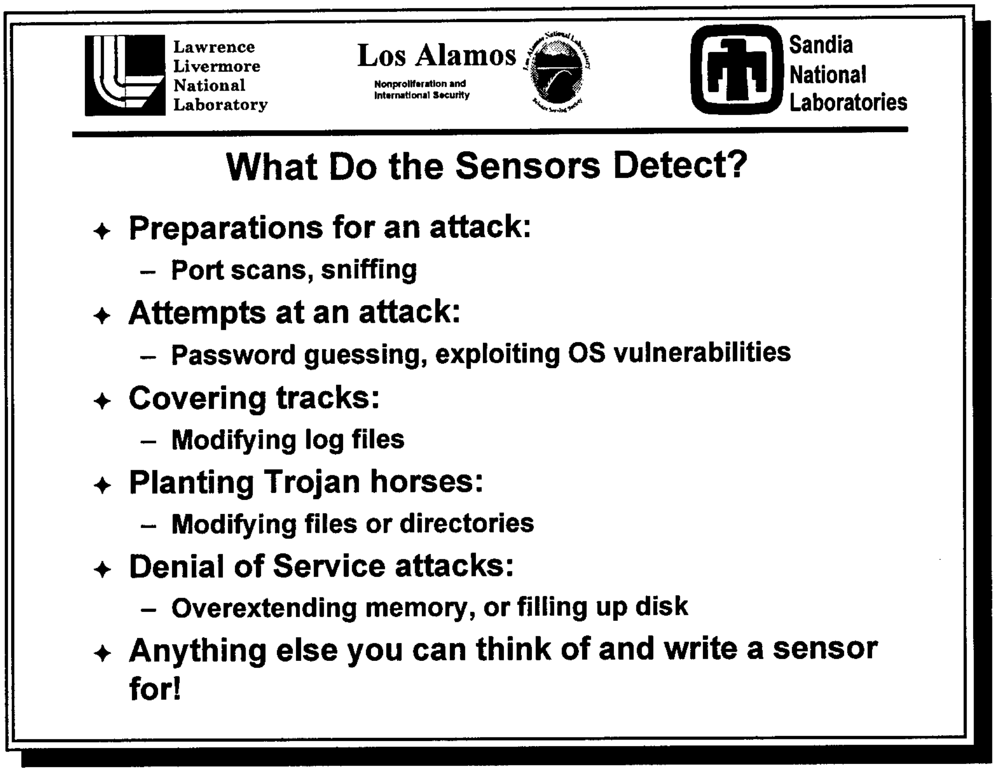
Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

Responses Vary in Aggressiveness: The Appropriate Response Depends on the Severity of the Attack

Info responses:
- email
- pager

Active responses:
- eject intruder
- ramp-up



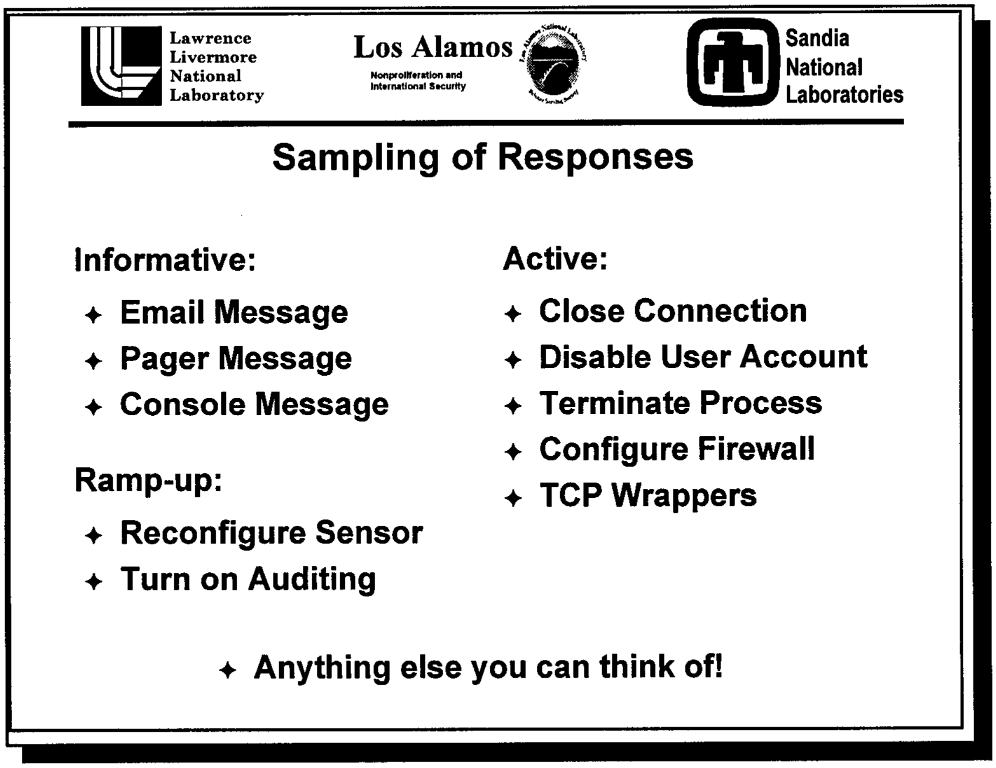
Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

What Do the Sensors Detect?

- Preparations for an attack:
  - Port scans, sniffing
- Attempts at an attack:
  - Password guessing, exploiting OS vulnerabilities
- Covering tracks:
  - Modifying log files
- Planting Trojan horses:
  - Modifying files or directories
- Denial of Service attacks:
  - Overextending memory, or filling up disk
- Anything else you can think of and write a sensor for!



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

Sampling of Responses

Informative:

- Email Message
- Pager Message
- Console Message

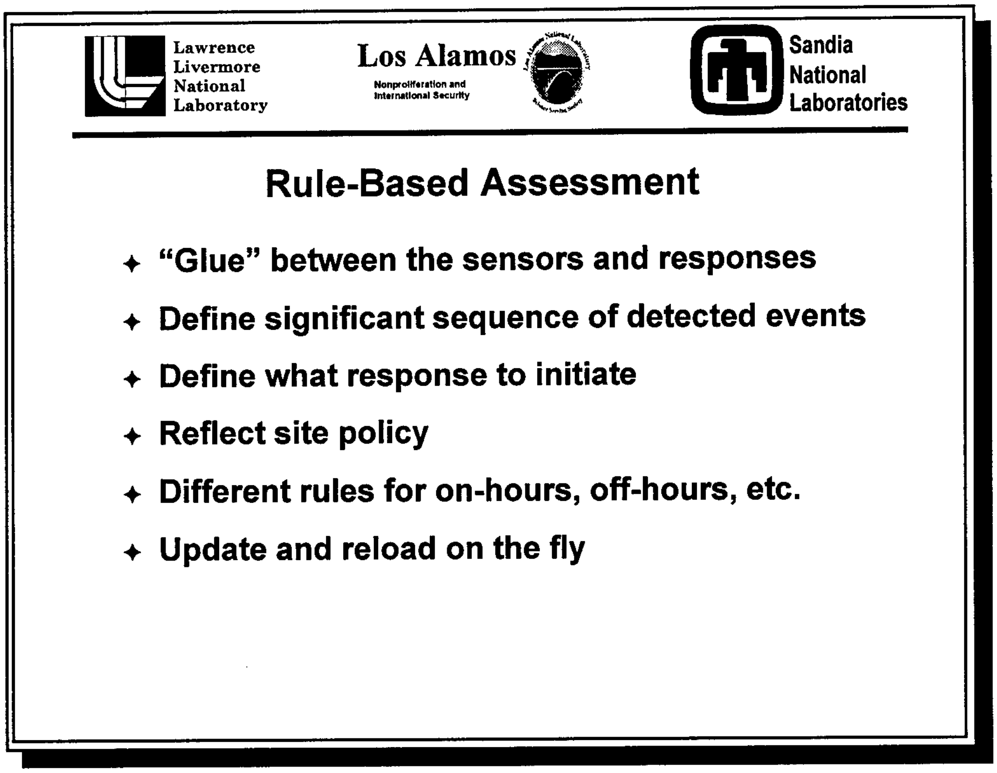
Ramp-up:

- Reconfigure Sensor
- Turn on Auditing

Active:

- Close Connection
- Disable User Account
- Terminate Process
- Configure Firewall
- TCP Wrappers

- Anything else you can think of!



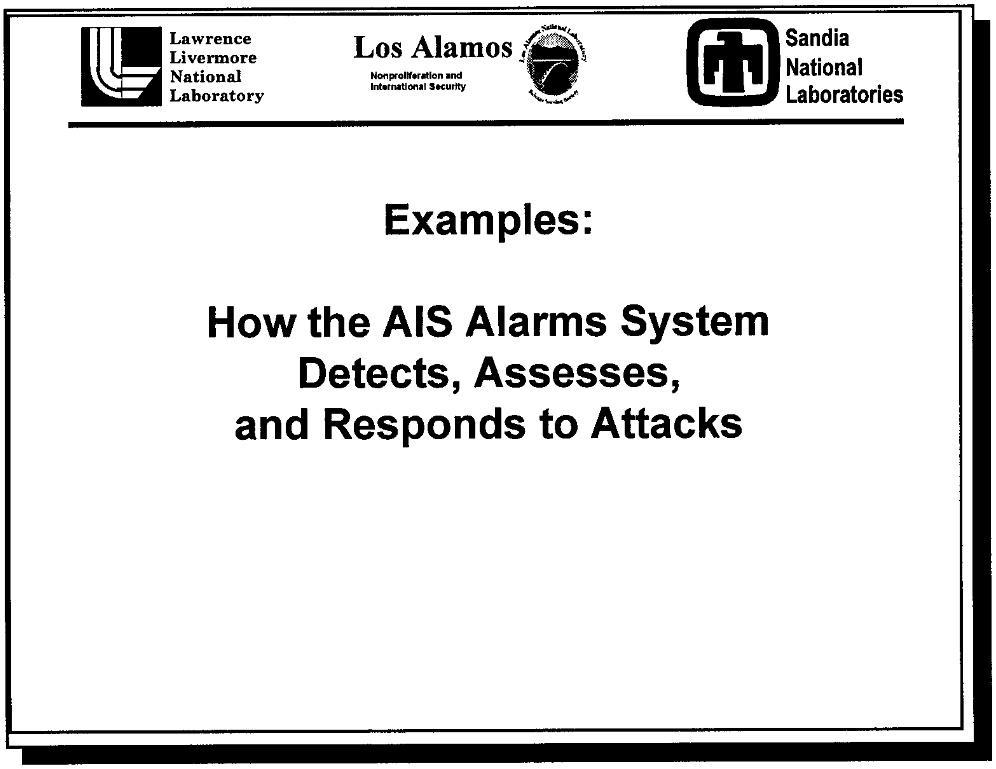
Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

Rule-Based Assessment

- "Glue" between the sensors and responses
- Define significant sequence of detected events
- Define what response to initiate
- Reflect site policy
- Different rules for on-hours, off-hours, etc.
- Update and reload on the fly



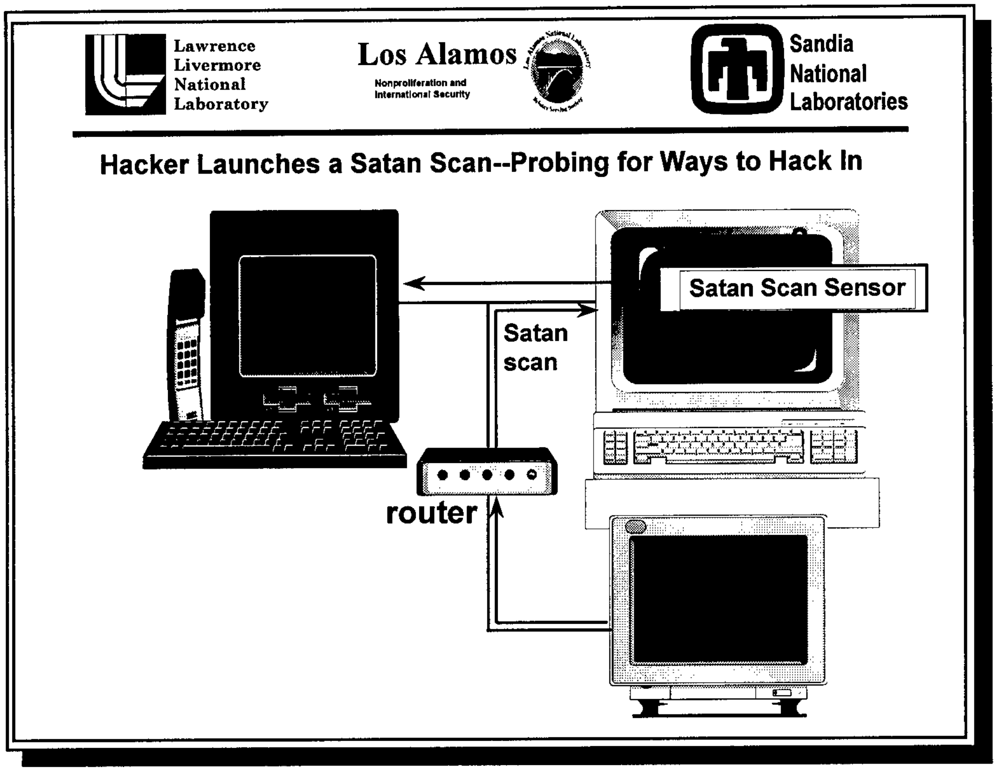
Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

Examples:

How the AIS Alarms System Detects, Assesses, and Responds to Attacks

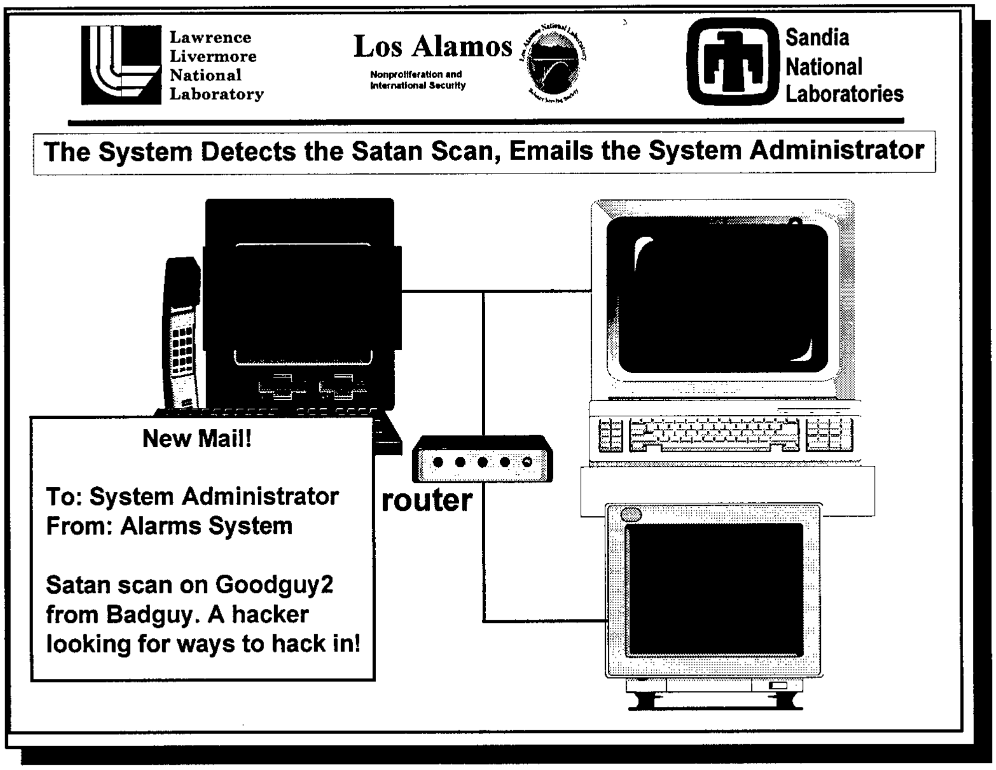


Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

Hacker Launches a Satan Scan--Probing for Ways to Hack In



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

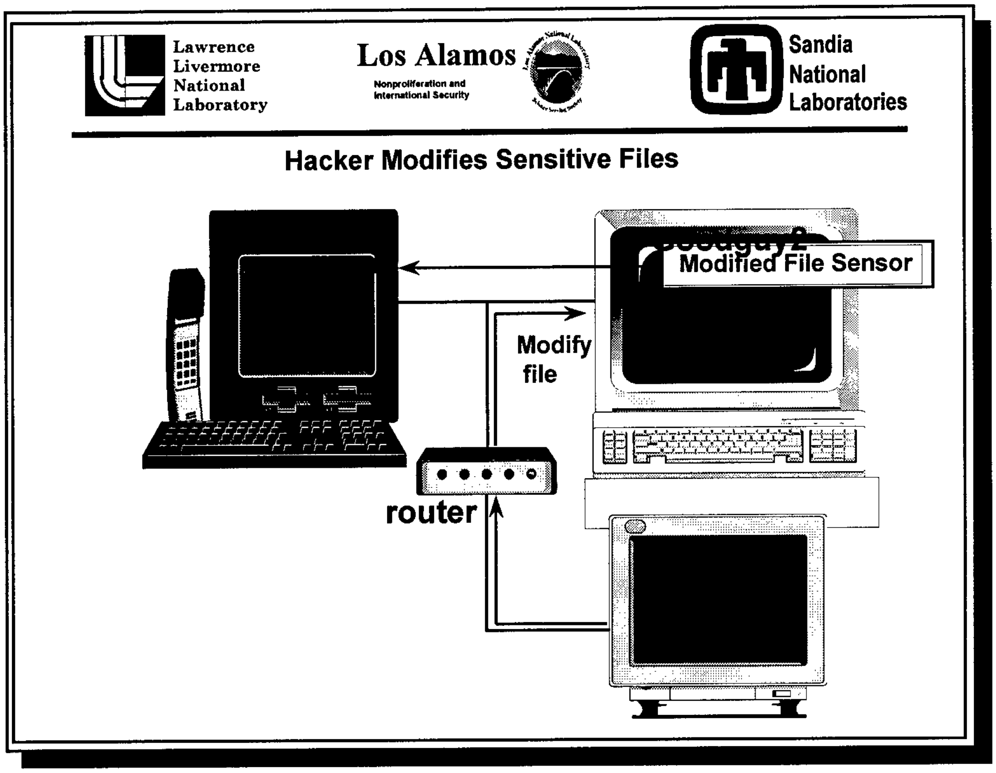
Sandia National Laboratories

The System Detects the Satan Scan, Emails the System Administrator

New Mail!

To: System Administrator
From: Alarms System

Satan scan on Goodguy2 from Badguy. A hacker looking for ways to hack in!

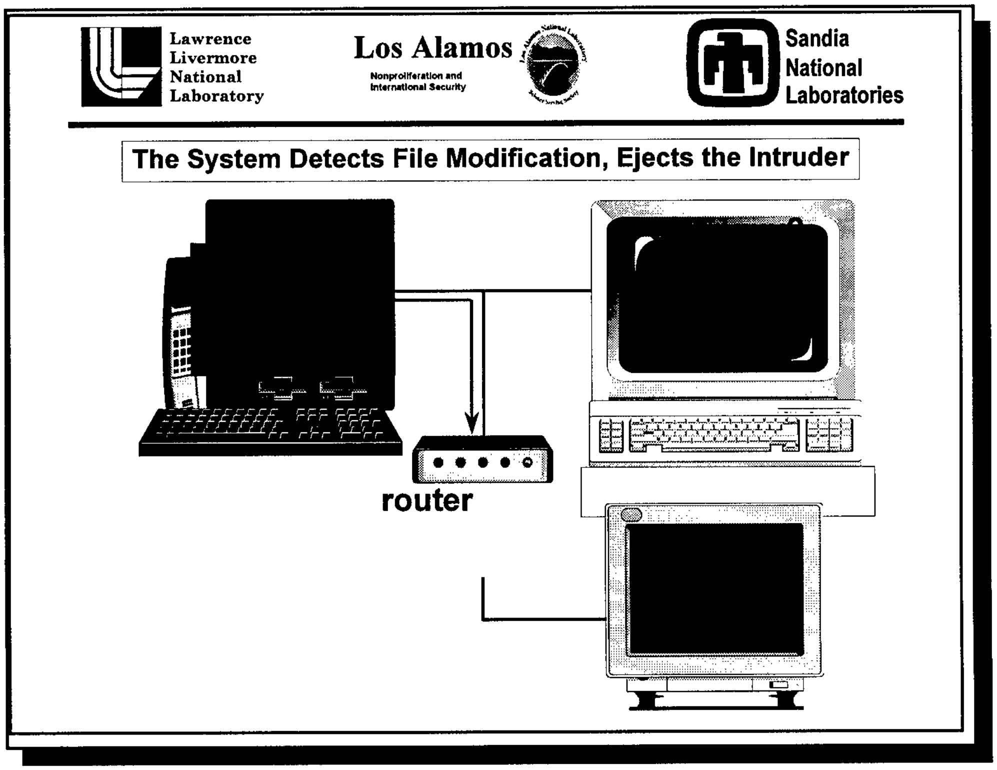


Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

Hacker Modifies Sensitive Files

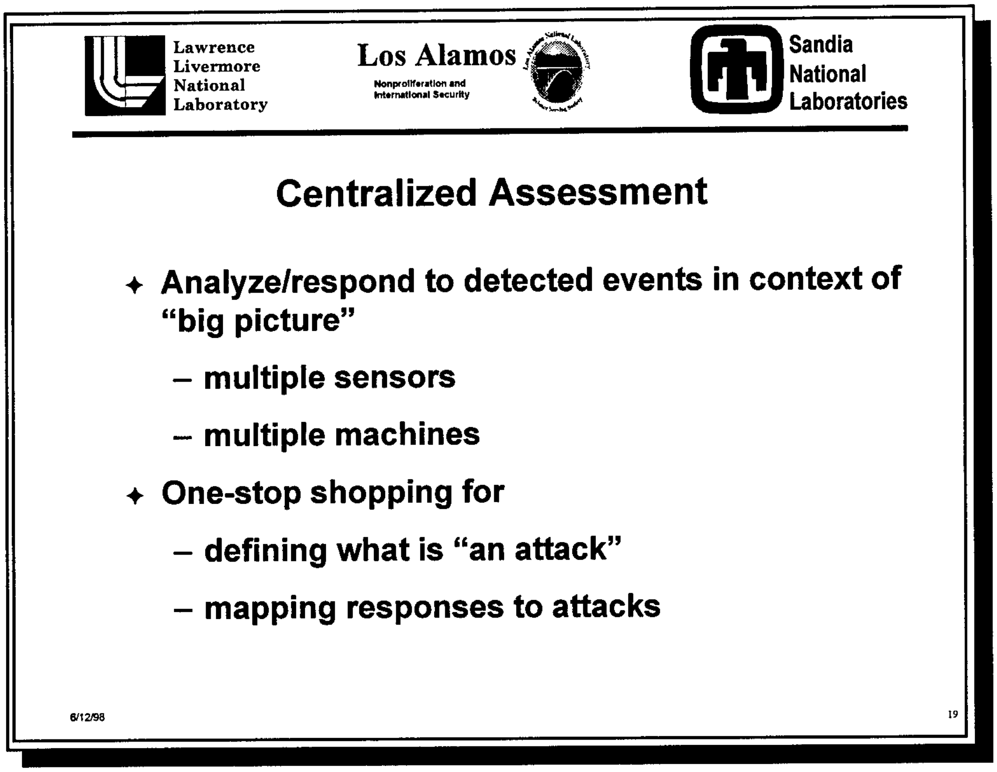


Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

The System Detects File Modification, Ejects the Intruder



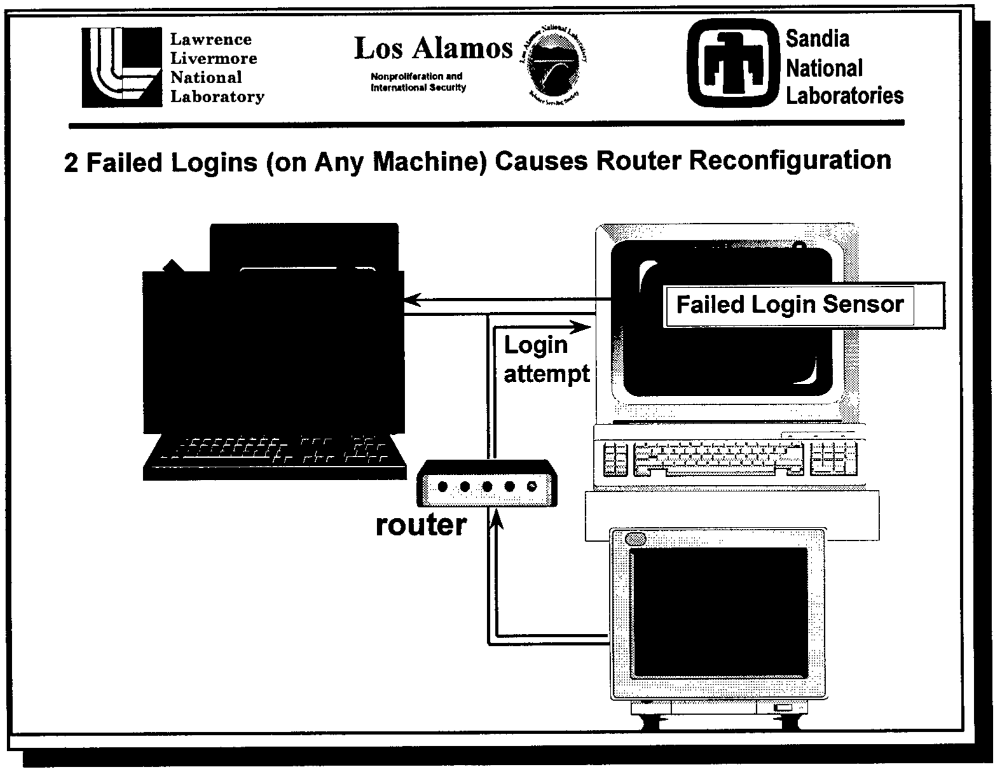
Lawrence Livermore National Laboratory
Los Alamos Nonproliferation and International Security
Sandia National Laboratories

Centralized Assessment

- Analyze/respond to detected events in context of "big picture"
  - multiple sensors
  - multiple machines
- One-stop shopping for
  - defining what is "an attack"
  - mapping responses to attacks

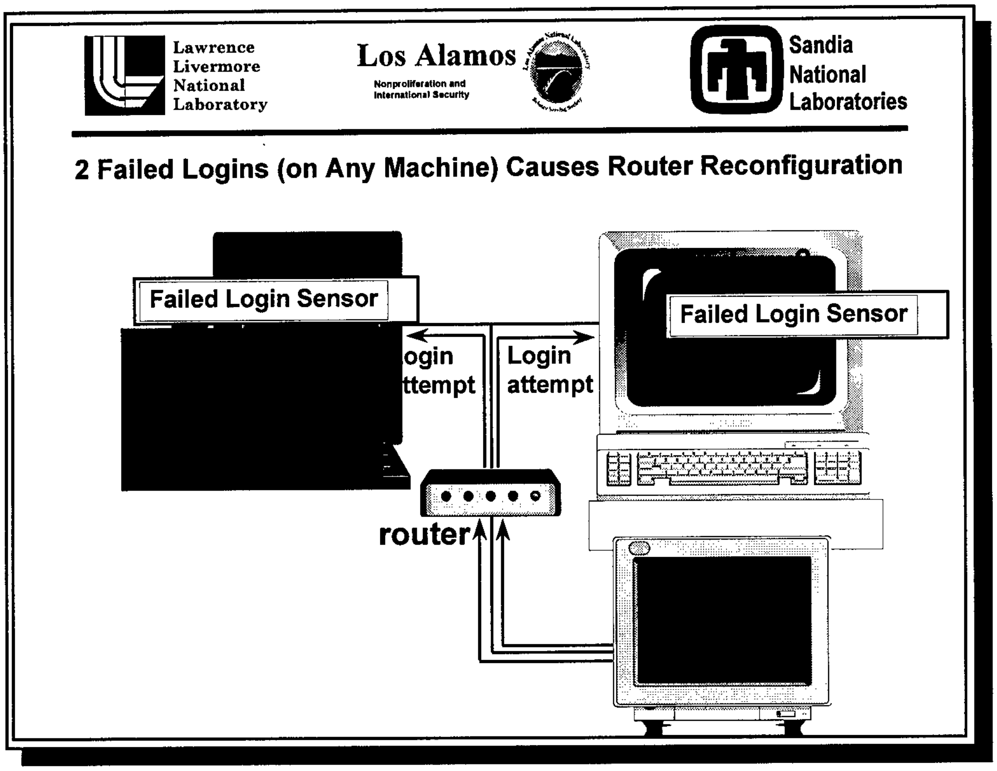
6/12/98

19



Lawrence Livermore National Laboratory
Los Alamos Nonproliferation and International Security
Sandia National Laboratories

2 Failed Logins (on Any Machine) Causes Router Reconfiguration



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

2 Failed Logins (on Any Machine) Causes Router Reconfiguration

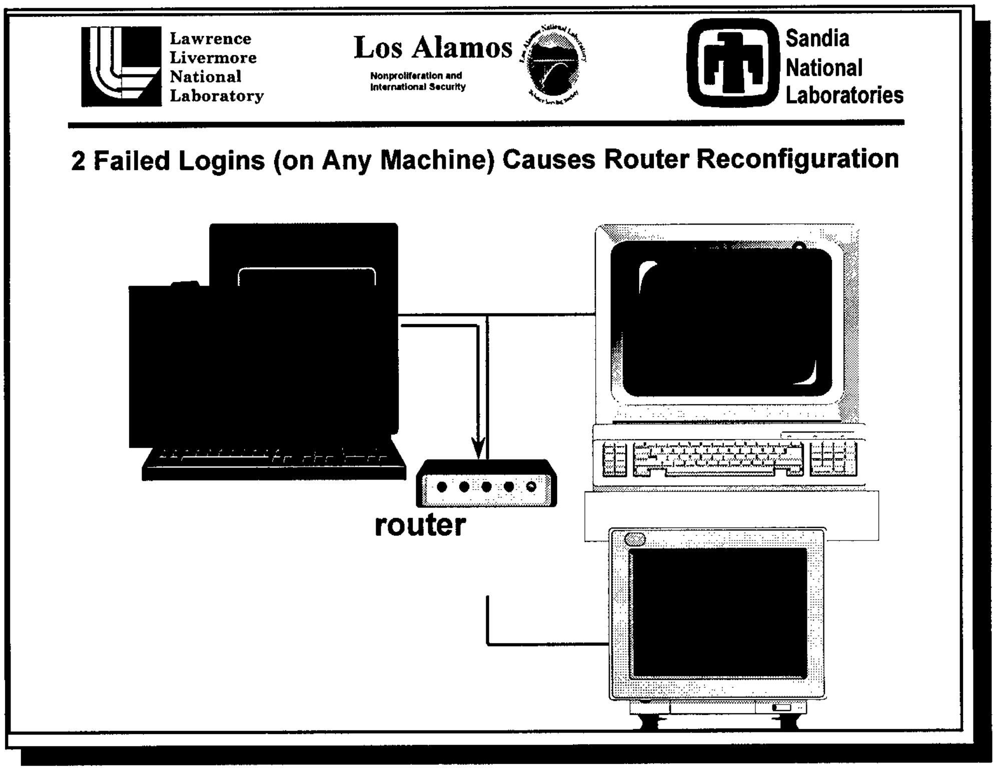
Failed Login Sensor

ogin
ttempt

Login
attempt

Failed Login Sensor

router



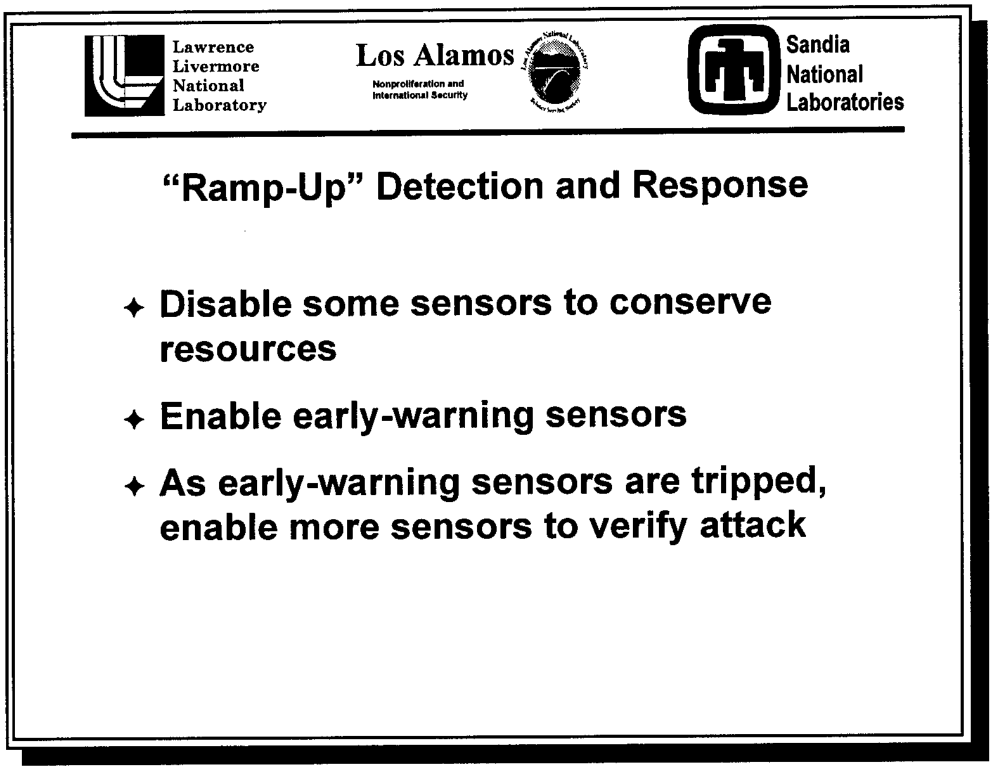
Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

2 Failed Logins (on Any Machine) Causes Router Reconfiguration

router



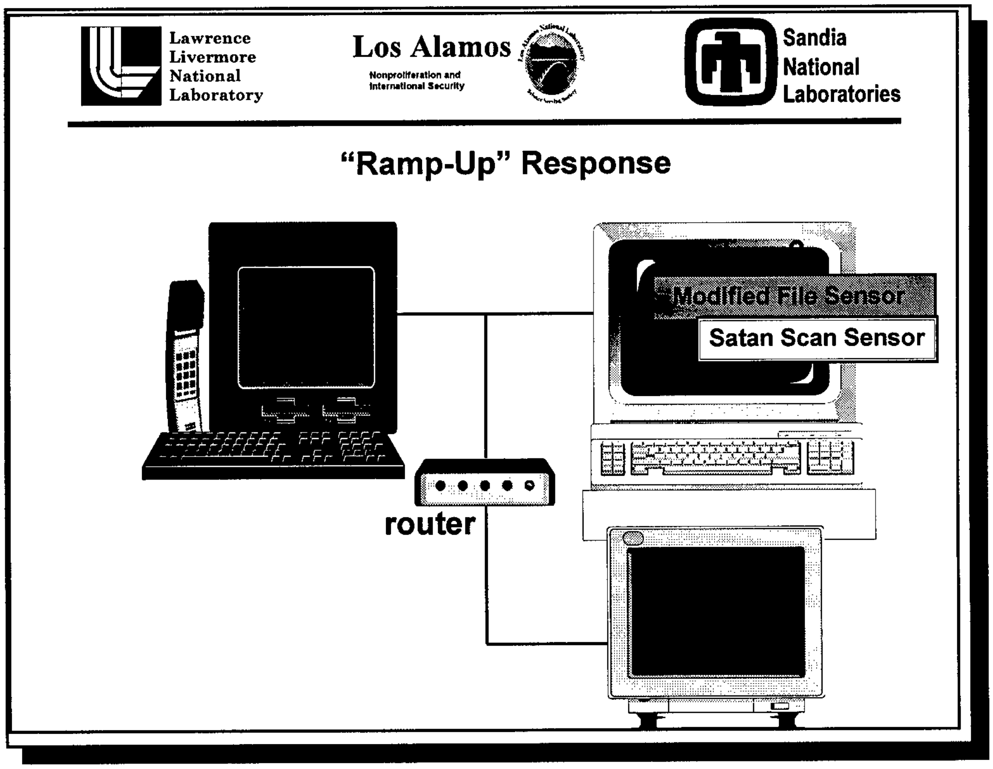
Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

"Ramp-Up" Detection and Response

- Disable some sensors to conserve resources
- Enable early-warning sensors
- As early-warning sensors are tripped, enable more sensors to verify attack

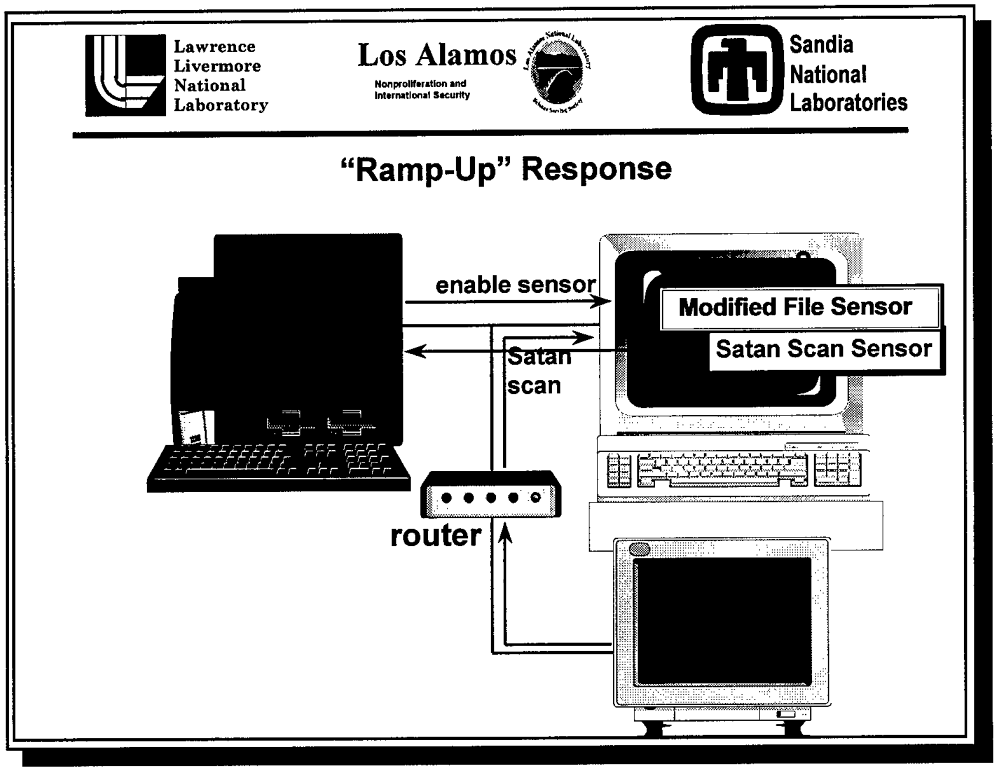


Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

"Ramp-Up" Response

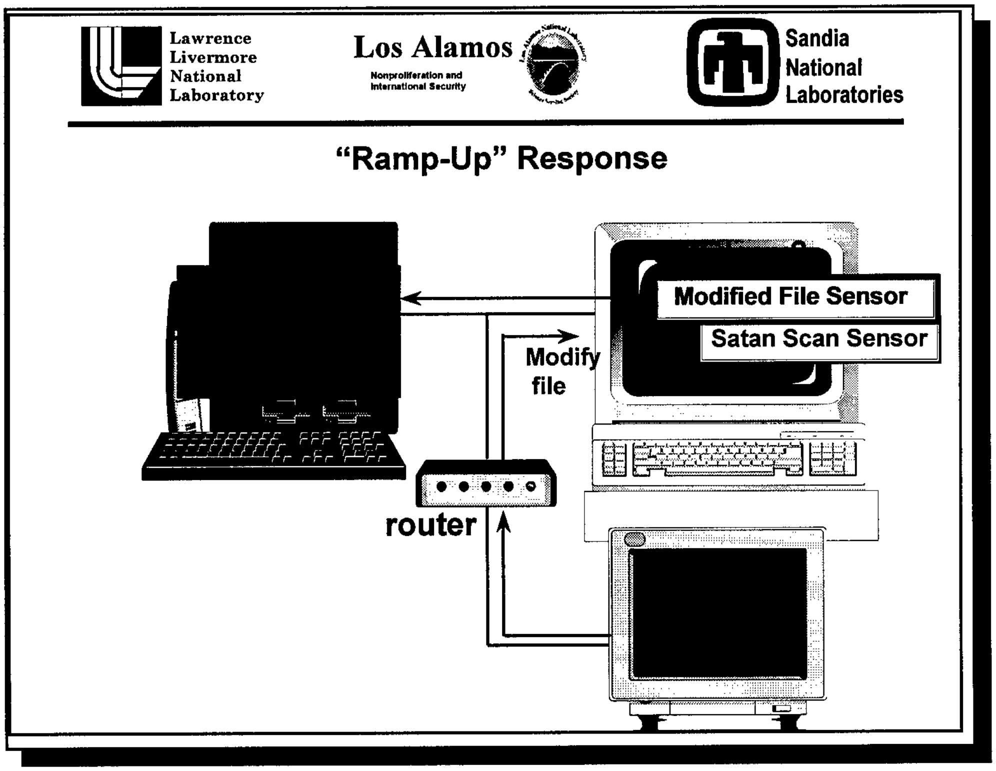


Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

"Ramp-Up" Response

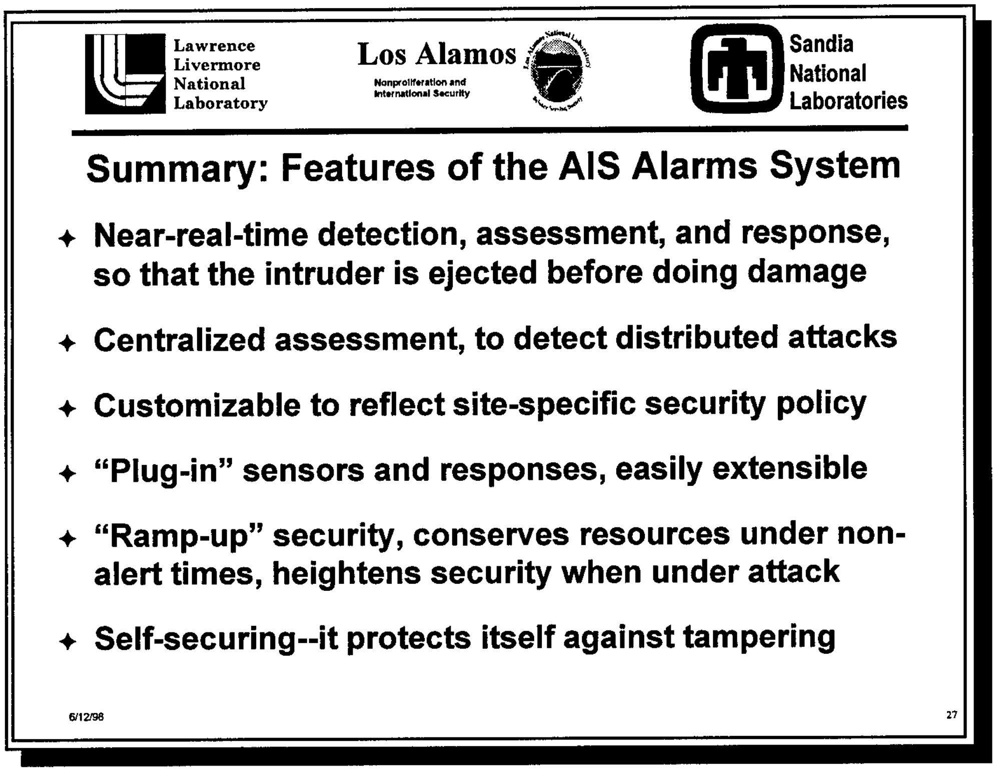


Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

"Ramp-Up" Response



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

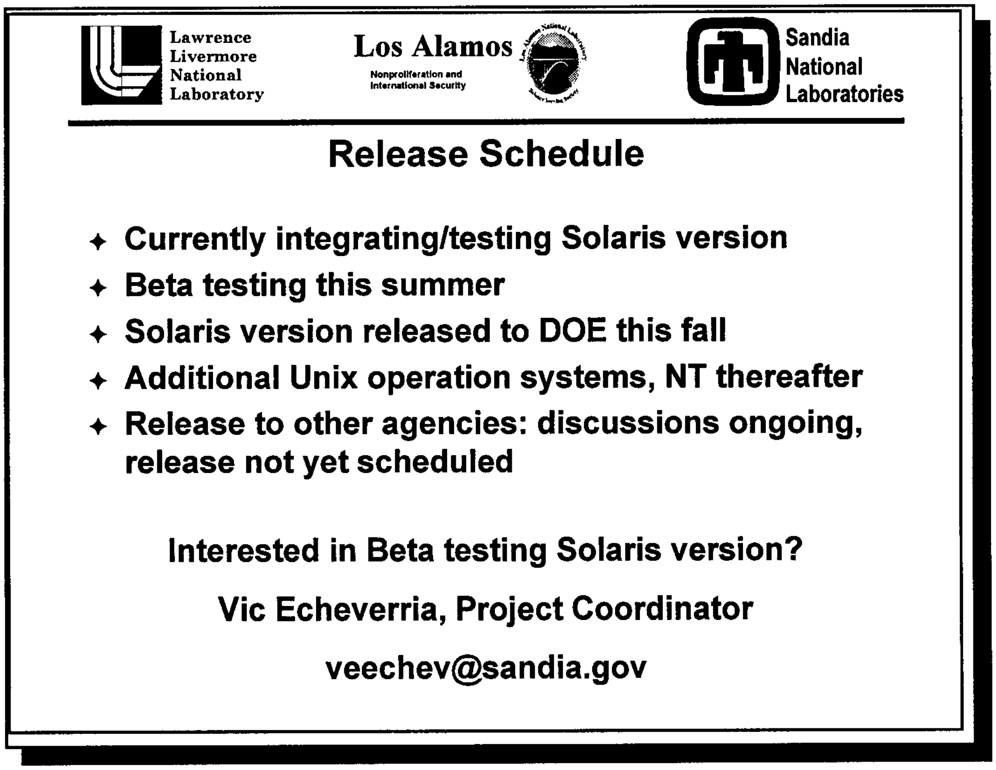
Sandia National Laboratories

Summary: Features of the AIS Alarms System

- Near-real-time detection, assessment, and response, so that the intruder is ejected before doing damage
- Centralized assessment, to detect distributed attacks
- Customizable to reflect site-specific security policy
- "Plug-in" sensors and responses, easily extensible
- "Ramp-up" security, conserves resources under non-alert times, heightens security when under attack
- Self-securing--it protects itself against tampering

6/12/98

27



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

Release Schedule

- Currently integrating/testing Solaris version
- Beta testing this summer
- Solaris version released to DOE this fall
- Additional Unix operation systems, NT thereafter
- Release to other agencies: discussions ongoing, release not yet scheduled

Interested in Beta testing Solaris version?

Vic Echeverria, Project Coordinator

veechev@sandia.gov

Persistent Access Control
or
How to retain control of your information even after distributing it

Paul B. Schneck

MRJ Technology Solutions

(703-277-1618, schneck@mrj.com)

Abstract

A revolutionary invention (patent pending) provides an information owner with the ability to retain control *after distribution* over who may use his information and how it may be used and redistributed. Intelligence reports, imagery, technical data, business information, movies, and audio recordings are but a few examples of the kinds of information that will be protected by this technology. Most importantly, this capability can be delivered in a standard personal computer, allowing users to utilize standard software. This solution, when available as a commercial, off-the-shelf product that provides security and access control is expected to become ubiquitous—a de facto standard for protecting all forms of digital information.

Background

Until recently, protecting some forms of information was relatively simple. Paraphrasing Marshall McLuhan, "The message is in the medium." Copying information required access to the technology used to package the information in the medium. Printed material, photographs, sound recordings, and movies could not be copied easily, could not be copied inexpensively, and certainly could not be copied covertly in an office environment. The widespread availability of xerographic copiers sent a warning signal that technological innovation could remove the barriers to copying. A scant two decades later the ubiquitous personal computer has made it possible for anyone to copy and distribute any digital file. At the same time, the medium is no longer important. Virtually all information types (audio, video, image, text, data, etc.) are now represented as digital data—strings of ones and zeroes—ready for processing by personal computers. The medium on which the bits are delivered, whether tape, magnetic disk, optical disk, telephone line, or other technology, is of no consequence for any subsequent use or processing.

In today's digital world, the source of a string of bits is irrelevant to the personal computer. The string can be processed, copied, or distributed at the touch of a few keys. Even the notion of a "copy" has changed. When dealing with two identical strings of bits (which are intangible) calling one a "copy" and the other the "original" is a distinction without a difference. That is why, when we purchase or license software we often receive a separate token of ownership: the bits are too easily copied.

Previous methods of control

Before the age of copier technology (xerography, personal computing) several approaches proved reasonably effective in controlling access. In the next few paragraphs we shall take a brief look at these approaches.

"Uncopyable" Media

The earliest examples of art, cave-dwellers' drawings, are inherently uncopyable. The best we can do is take a picture and reproduce a two-dimensional image, without the texture or the environment. Prior to the invention of the printing press hand printed documents were "effectively" uncopyable. Our use of a hand-written signature to execute a binding contract is a remnant of the view that an individual's signature is an original that cannot be copied. Even today, so-called "coffee-table books" are testimony to the fact that xerographic copies, although they may be capture many apects, do not capture every aspect of the original. How many times have you seen a coffee-table photocopy?

Many personal computer software manufacturers attempted to protect their products by distributing them on "uncopyable" media. As they soon found out, many consumers rose to the challenge and developed techniques for copying these media and, because "bits are bits", the copies worked just as well as the originals.

Legal and Administrative Controls

The early Hebrew liturgy contains many examples of poetry in which the author's name is embedded, for example as the first letter of each line. Copying the poem brings the author's name along. It would be difficult if not impossible to remove the author's name without damaging or diminishing the original poem. This technique foreshadows the use of "watermarks" or embedded signaling to identify the owner of audio or video information.

The Statute of Anne provided specific printers the sole rights to produce and publish written materials. Modern copyright laws developed from this early example. Today copyright law generally provides that the copyright holder has a property interest in his information. That is, he may act to prevent anyone else from copying or selling the information, subject to the specifics of the law.

The use of administrative techniques is subject to the degree of control that the administrative system can exert on the user. This varies depending on the specifics of each situation. Even in the best cases, administrative controls can be flouted by a criminal or undermined by careless or negligent behavior.

Encryption

The mathematics of encryption allows one to scramble a message so that it can only be unscrambled by another individual possessing the appropriate "key". This process can be carried out to provide as high a degree of assurance against eavesdropping as is necessary. For example, someone attempting to decrypt a message that was encrypted with a 128-bit key, using one billion personal computers (more than all those ever manufactured) operating at one trillion decryption attempts per second (tens of thousands of times faster than microprocessors that are being designed today) would require over a trillion years. The universe is about 15 billion years old, only one 60th of the time required!

However, once the message is unscrambled and in the recipient's possession it is just a string of bits. We must trust the recipient to safeguard the information. Encryption can only safeguard the delivery or first access to information. It cannot provide enduring control.

Handling of Classified Information

The security of certain classified information is ensured by the use of an administrative control system and a physical control system. The administrative control system vets all individuals who will have acess to classified information. It also puts in place procedures (such as the "two-person rule") for ensuring that a lone individual will not have the opportunity to deviate from the rules. The physical control system provides for secure facilities of processing information and packages and safeguards information in transit between facilities.

The philosophy of the system is that information can only be processed in a secure facility and cannot be removed from the facility without being packaged for secure delivery.

Persistent Access Control

Concept of Operations

Protecting/Packaging

Information that an owner wishes to protect is packaged by the owner and made available to users and potential users. Encryption is one of the packaging steps. This allows the information to be transmitted and distributed without concern that it will be accessed without authorization.

The owner or his representative may send packaged information to users and potential users (the "push" model). Alternatively, the owner may place packaged information on a server in order that users can download it (the "pull" model).

Licenses

Packaged information can be accessed only under the control of a corresponding license. The user or representative prepares a license for each user. Each license specifies the access privileges available to the user. Licenses are themselves protected by encryption (using the public key of the recipient's computer).

Licenses may be distributed with data, to each user on the distribution list or may be prepared and sent in response to users' requests.

Secondary recipients of protected files must contact the owner/representative in order to obtain a license for access

If the owner/representative chooses, a license can authorize specific recipients to distribute copies or derivative products and to provide licenses, perhaps with limited access privileges, to additional recipients.

A small infrastructure is required to validate the authenticity of the public key to be used to encrypt a license. This can be a centralized repository or can be distributed and implemented as the responsibility of the content owner—who has the greatest interest in ensuring protection. If desired, the computer owner's identity can be associated with a key.

The Computer

A modified computer, containing some additional hardware and software is used to ensure access control in accord with the user's license. The modified computer is compatible with current files. Existing software can be used with current files or with new, protected files.

The modifications include changes to the BIOS to implement an access control mechanism that mediates all input and output operations; a place for storing the computer's private key; and a tamper-detecting enclosure. The tamper-detecting enclosure causes the private key to be erased in the event tampering occurs. When the private key is erased, the computer can no longer access any protected files although it can continue to be used to process current (unprotected) files.

The User

There are no differences in operation when accessing unprotected files. Application programs need not be aware of this new capability. They can continue to operate unchanged when working with unprotected files. When the user's program attempts to access (read) a protected file the system will search for a corresponding license. If none is found, the system will ask the user to locate a license or to terminate the program (similar to what occurs if attempting to read the floppy disk drive when no disk is present). After the license is located the system check the access rights granted to the user. Only if the license allows access will the file be read, decrypted, and made available to the application—which is unaware that these access control operations are taking place. If access is not permitted, the program will receive an error indication or will be terminated.

A similar process takes place when the user's program attempts an output (write) operation. The license is consulted to determine whether or not output is allowed and what restrictions may apply (e.g., force "watermarking", restrict to black and white, restrict resolution, etc.). If multiple protected files are in use the system enforces the intersection of the restrictions of all active licenses. This is equivalent to operating at "system high".

"Aware" Programs

The access control mechanism can return a license parameter to a program that makes an inquiry. This allows programs aware of the access mechanism to offer variable levels of features to users, depending on the license that is present.

This new capability allows a software creator to package multiple versions in one release and to license individual capabilities to end-users.

User Identity

As described so far, licenses and access privileges are tied to a specific computer. The implementation can easily allow use of a "smart card" or other token so that licenses can be tied to a specific user—either on a particular PC or on any of a pool of PCs—allowing intra-enterprise “nomadic computing”.

Conclusion

This invention provides continuing control over access to data, even after they are distributed. Copies of protected files, as well as derivative files (those based on input from protected files) all need authorization of the owner of the original file before a user can obtain access. At no point can a digital copy be made without the owner’s authorization.

The President's National Security
Telecommunications Advisory Committee

A Model of Industry and Government Partnership

Mr. Guy Copeland
Computer Sciences Corporation
3170 Fairview Park Drive, Falls Church, VA 22042
Tel: 703-641-2561 Fax: 703-849-1005
EMail: gcopelan@csc.com

NSTAC Info: http://www.ncs.gov/nstac.htm
NSTAC Secretariat: 703-607-6209

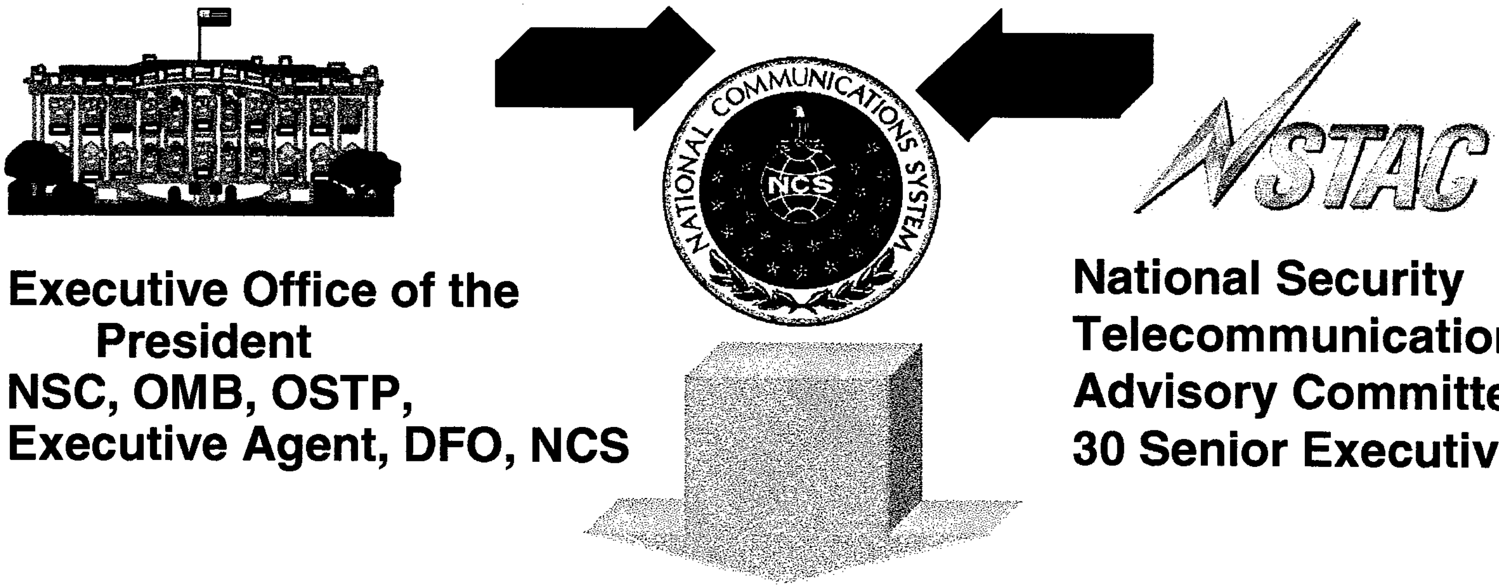
Agenda

- NSTAC Background
- Critical Infrastructure Risk Assessments
  - Telecommunication
  - Electric Power
  - Financial Services
  - Transportation
- National Coordinating Mechanism
- Questions

NSTAC Formation

- Established: President Ronald Reagan, Executive Order 12382, September 1982, as amended
- Authority: Federal Advisory Committee Act
- Executive Agent: William Cohen, Secretary of Defense
  - Designated Federal Official: LTG David Kelley, Manager, National Communications System (NCS) & Director, Defense Information Systems Agency (DISA)
  - Up to 30 CEOs
    Telecommunications and Information Industries
- Chair: Currently Mr. Charles R. Lee, GTE
- Vice Chair: Currently, Mr. Van B. Honeycutt, CSC.

Joint Government/Industry Partnership



Executive Office of the President
NSC, OMB, OSTP,
Executive Agent, DFO, NCS

National Security
Telecommunications
Advisory Committee
30 Senior Executives

NS/EP Telecommunications and Information Systems

15 Years of NSTAC Results

- National Coordinating Center (NCC) for Telecommunications
- International Diplomatic Telecommunications
- Electromagnetic Pulse (EMP) Assessment
- Commercial Network Survivability (CNS) Assessment
- Telecommunications Industry Mobilization (TIM) Assessment
- Commercial Satellite Survivability (CSS) Assessment
- Telecommunications Service Priority (TSP)
- Network Security Information Exchange (NSIE)
- Enhanced Call Completion (ECC)
- Cellular Priority Access Service (CPAS)
- Government Emergency Telecommunications Service (GETS).

National Coordinating Center for Telecommunications (NCC)

- Established 1984
- Industry members: AT&T, COMSAT, GTE, ITT, MCI, NTA, Sprint, Worldcom, USTA
- Government members:
  - Departments of Defense, Energy, Justice and State
  - Agencies: FCC, FEMA, GSA
- Assists in initiation, coordination, restoration and reconstitution of NS/EP telecommunications services or facilities (under all conditions, crises, or emergencies)
- Exercises, response planning, training
- Examining expanded future role (I&W, NCM)
- Successful model for daily industry/government partnership

Network Security Information Exchange

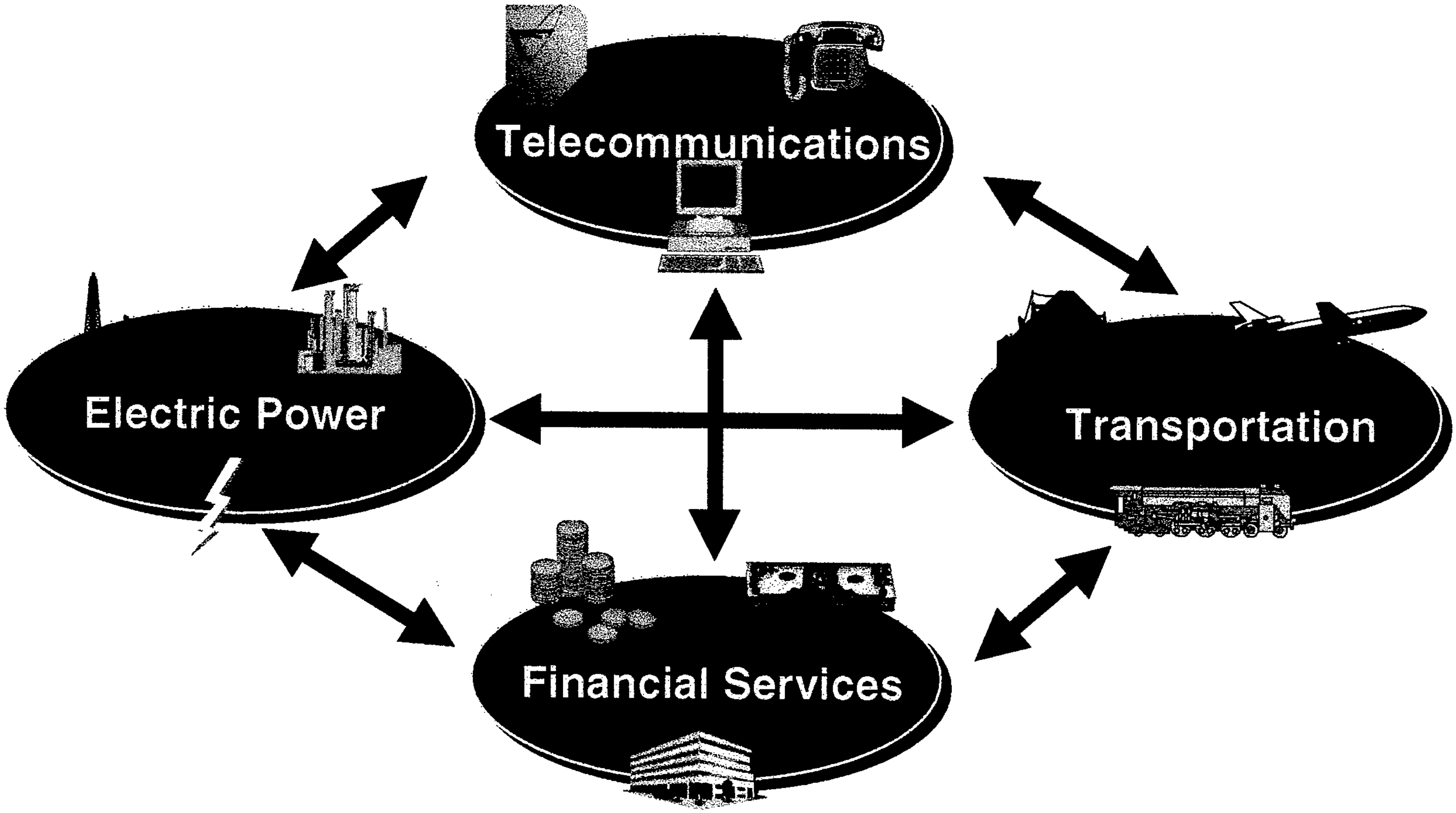
- Growing Vulnerability of the Public Switched Network, NRC, 1989
  - "...NCS should consider how to protect the public networks from penetration by hostile users..."
- April 1990, NSC memo to Manager, NCS
  - ... the 'hacker' threat."
- Our opponents were sharing information, why not us?
- Based on Bellcore's Security Information Exchange
- First meeting June 1991; 40th meeting March 1998
- Members 1991: 9 Government; 9 NSTAC
- Members 1998: 10 Government; 20 NSTAC

NATIONAL SECURITY TELECOMMUNICATIONS • ADVISORY COMMITTEE •

NSTAC

Critical Infrastructure Risk Assessments

Critical Infrastructure Interdependence



Telecommunications Risk Assessment

Telecommunications Risk Assessment

- "An Assessment of the Risk to the Security of Public Networks"
- Prepared jointly by Government and Industry Network Security Information Exchanges
- NSIE's update periodically
- Available through the Office of the Manager, National Communications System

Telecommunications - Conclusions

- Overall risk to the public network is greater than reported in the 1993 risk assessment
- Reliance on the public network is growing
- Complexity of the network (technology, interfaces, size, etc.) is growing
- Threats are outpacing deterrents
- Vulnerabilities are outpacing the implementation of protective measures

Telecom Industry's Top Security Concerns

- Increased number of access points and networking
- Collocation of carriers into one carrier's infrastructure basket(s)
- Increased number of interconnected inexperienced systems administrators and processes
- Embedded Operations Channels of PTN Signaling and Transport Protocols (e.g., SONET DCC, ATM OAM Cells, SS7 Network Management Messages) gives virtually unlimited access to everything and everyone connected (networked) to them
- Internet and Intranet Exploitable technology used for access to Network Operations and Signaling Systems
- Local Number Portability Added complexity, dependencies and single points of failure
- Lack of Fidelity Bonds, Criminal Background Checks
- CALEA Control Requirements of Section 229 of the Act

Network Reliability and Interoperability Council, 4/97

Public Switched Network Security

"Within the PSN, intruders have already compromised nearly all categories of activities, from switching systems to operations, administration, maintenance, and provisioning (OAM&P) systems, and to packet data networks. Private branch exchanges (PBXs) and corporate networks that tie into the public network have crashed or disrupted signal transfer points (STPs), traffic switches, OAM&P systems, and other network elements. They have planted destructive 'time bomb' programs designed to shut down switching hubs, disrupted E-911 services throughout the eastern seaboard, and boasted that they have the capability to bring down all switches in Manhattan."

Reliability and Vulnerability Working Group, IITF

Electric Power Risk Assesment

Electric Power - Key industry trends

- Shift from:
  - Proprietary control protocols to Utility Control Architecture
  - Mainframe applications to client-server
  - Isolated control centers to interconnections
  - Manual on-site maintenance to remote substation automation
- FERC rulemaking on open access to transmission system information (OASIS):
  - Forcing utilities to separate transmission control from power marketing
  - Utilities will post transmission system information on Internet web hosts
- Deregulation will lead to major industry restructuring
- Increased competition inhibits information sharing

Electric Power - Observations

- Control centers and control center computers today are relatively isolated from public networks
  - Use of private networks for transport
  - Limited or no connectivity with corporate networks
  - Multiple operational checks within control applications
  - Remote maintenance access by EMS vendors is the primary vulnerability

Electric Power - Observations (2)

- Substation automation is source of most exposure
  - Maintenance/administration ports on:
    - Remote Terminal Units (RTU's)
    - Protective relays
    - Circuit breakers
  - Widespread reliance on dial-up access
  - Rudimentary access controls
  - Combined with simple critical node analysis, could allow simple attack to cause major network outage

Electric Power - Information security

- Information security awareness just beginning to mature
  - Proliferation of modems on network-attached PCs
  - Simple dial-back access controls on modem pools
  - Virus response programs
  - Limited network password/ID management
  - Less than half the companies interviewed have a focal point for information security
- Physical threats (weather, natural disasters, vandalism) far outweigh network-based threats
- Consistent interest in:
  - Mechanism for incident/vulnerability/threat information exchange
  - Providing threat awareness briefing to senior managers

NATIONAL SECURITY TELECOMMUNICATIONS • ADVISORY COMMITTEE

NSTAC

Financial Services Risk Assessment

Financial Services Objectives

- Assess the security and robustness of the financial services infrastructure at the national level relative to the identified threats to its networks and information systems
- Determine the risks to the financial services industry that derive from its dependence on information technology and the telecommunications infrastructure
- Examine the implications of trends regarding the industry's use of information systems and networks.

Conclusions

- Perceptions vs. reality
  - Citibank was NOT a hack
  - Hackers/experts perpetuate
  - *Debt of Honor*, Tom Clancy
- Natural disasters and physical attacks
  - Few single points of failure
  - Considerable experience
- Cyber Risks
  - Year 2000 biggest challenge
- Cyber Threats
  - Reluctance to share (on all sides)

Findings

- U.S. financial services infrastructure is well protected to withstand all but a full-scale, national-level attack
- Security is fundamental consideration
  - Accountability and oversight to the board level
  - Integral element of risk management
  - Major investments: security, diversity, backup, recovery
- Government needs to provide more threat information
- Consideration should be given to the monitoring of emerging electronic payment systems
- There is an issue on adequate background checks at hire.

Transportation Risk Assessment

Transportation

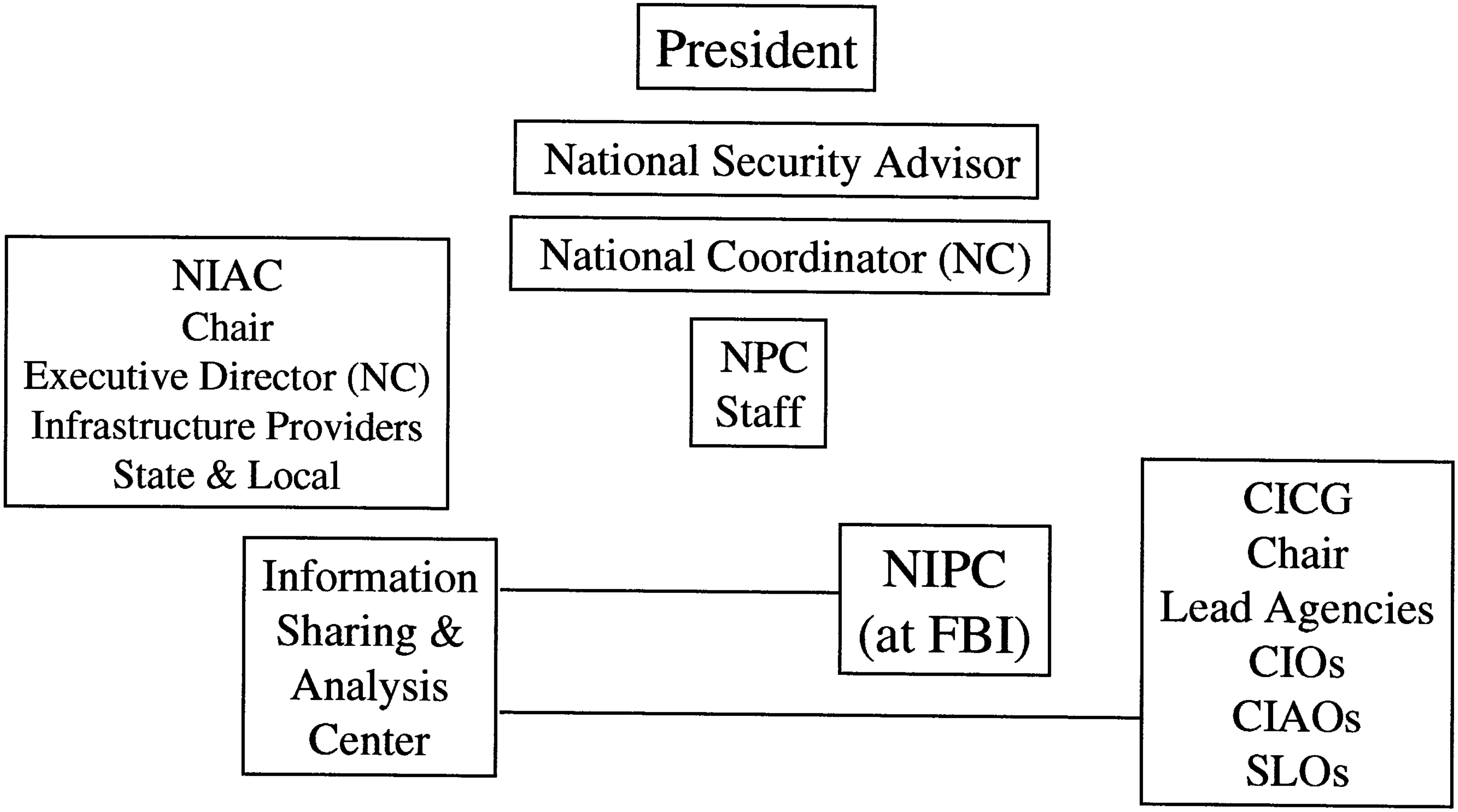
- Key elements of transportation infrastructure:
  - Air traffic control and airspace safety
  - Highway
  - Maritime
  - Rail
  - Trucking
  - Oil and natural gas pipelines
- Initial Workshop in Atlanta, September 10, 1997
- Interim report to NSTAC XX, December 11, 1997
- Continuing

Aside on Contacts with Industry

- Views on government involvement vary among individual industries, based on:
  - Existing information sharing and coordination mechanisms
  - Extent of regulatory controls
  - Experiences from other encounters

- However, industry is consistent in some views:
  - Suspicion of motivations for government involvement
  - Skepticism about threats
  - Concern about privacy and trust in any information exchange

PDD-63, May 22, 1998



President

National Security Advisor

National Coordinator (NC)

NPC
Staff

NIAC
Chair
Executive Director (NC)
Infrastructure Providers
State & Local

Information
Sharing &
Analysis
Center

NIPC
(at FBI)

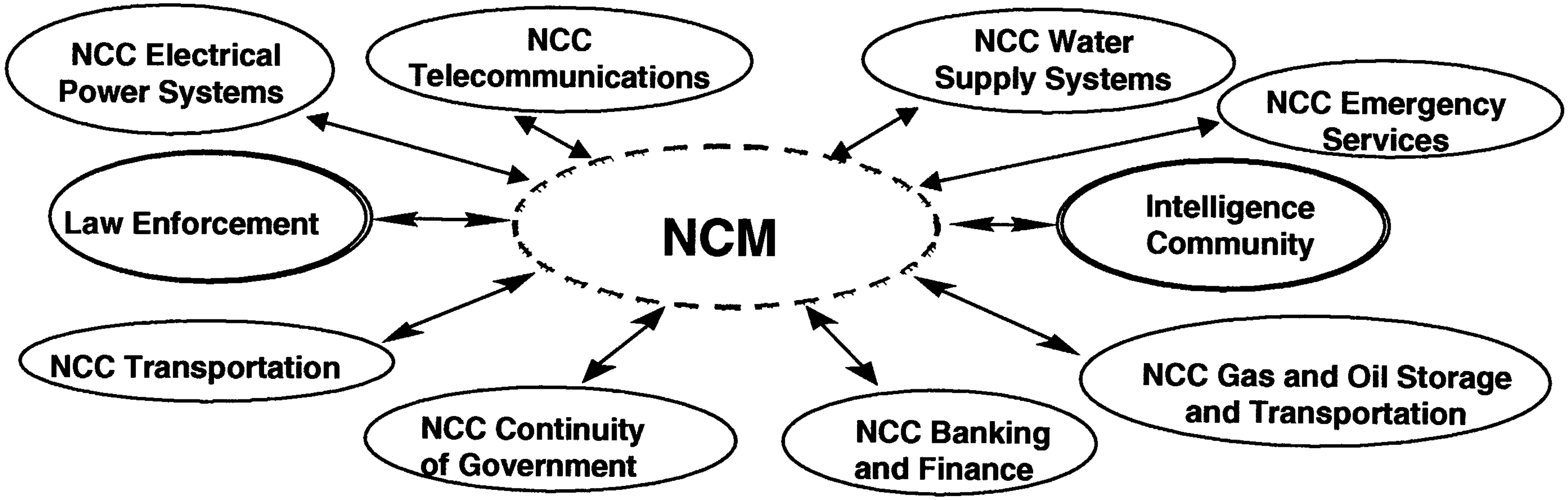
CICG
Chair
Lead Agencies
CIOs
CIAOs
SLOs

NATIONAL SECURITY TELECOMMUNICATIONS • ADVISORY COMMITTEE •
NSTAC

National Coordinating Mechanism (NCM)

National Coordinating Mechanism

The feasibility of the NCM depends on industry and Government's willingness to participate in the information-sharing process.



Reports

Many final reports can be found at:

http://www.ncs.gov/nstac/reports.html

Or by calling OMNCS at 703-607-6209

- Electric Power Risk Assessment Report
- Issue Review - December 1997
- Intrusion Detection Subgroup Report
- Information Infrastructure Group Report
- Financial Services Risk Assessment Report
- Legislative and Regulatory Group Report
- Operations Support Group Report.

NATIONAL SECURITY TELECOMMUNICATIONS • ADVISORY COMMITTEE •
NSTAC

Questions?

U.S. GENERAL SERVICES ADMINISTRATION

MELVIN L. BASYE

DIRECTOR, SECURITY DIVISION

OFFICE OF FEDERAL PROTECTIVE SERVICE

OVERVIEW OF PRESENTATION

- Federal Protective Service Mission
- How We Meet Our Mission Requirements
- Current Initiatives

FEDERAL PROTECTIVE SERVICE MISSION

The Federal Protective Service is charged with providing a safe and secure environment, that is open and inviting, in a cost effective, knowledgeable, professional, and sophisticated manner, permitting Federal agencies and members of the public to conduct their business without fear of crime or disorder

HOW WE MEET OUR MISSION REQUIREMENTS

- Basic Security
  - Contract Guards: Access Control, Monitoring, Foot Patrols
  - Maintaining 24 Hour Alarm Monitoring And Response Centers
  - Physical Security Surveys
  - Crime Prevention And Awareness Training
  - Assisting Building Security Committees
  - Coordinating/Developing Occupant Emergency Programs
- Building Specific
  - Repair And Maintenance Of Security Equipment
  - Amortization Of Capital Expenditures For Security Equipment

HOW WE MEET OUR MISSION REQUIREMENTS - CONTINUED

- Patrol And Response - 22 Core & Satellite Cities
  - Mobile Patrols - Crime Detection & Deterrence
  - Investigations On Reported Offenses & Incidents
  - First Responders To NBC Incidents
  - Coordination With Other Federal/State/Local Law Enforcement Agencies
  - Threat Analysis & Dissemination - Deter/Monitor Criminal/Terrorist
  - Assist In Development Of Emergency Contingency Plans
  - Monitor Alarms
- Patrol And Response - Non Core/Satellite Cities
  - FPS Physical Security Specialist
  - PFS Criminal Investigator
  - Contract Security Guards
  - Local Law Enforcement

CORE AND SATELLITE CITIES

- Core Cities
  - Washington, DC
  - Los Angeles/Long Beach
  - Chicago, IL
  - Philadelphia, PA - NJ
  - Kansas City, MO - KS
  - New York, NY/Newark, NJ
  - San Francisco/Oakland, CA
  - Denver/Boulder, CO
  - Atlanta, GA
  - Dallas/Ft. Worth, TX
  - Boston, MA
  - Seattle/Everett, WA

- Satellite Cities
  - Baltimore, MD
  - Albany/Schenectady/Troy, NJ
  - St. Louis, MO - IL
  - Detroit, MI
  - Houston, TX
  - Cleveland, OH
  - Portland, OR
  - New Orleans, LA
  - San Juan, PR
  - Miami, FL

CURRENT INITIATIVES

- Completion Of Security Enhancements
- Security Design Criteria
- Development Of Comprehensive Intelligence Program
- NBC Training For Security Force

QUESTIONS?

DEPARTMENT OF DEFENSE

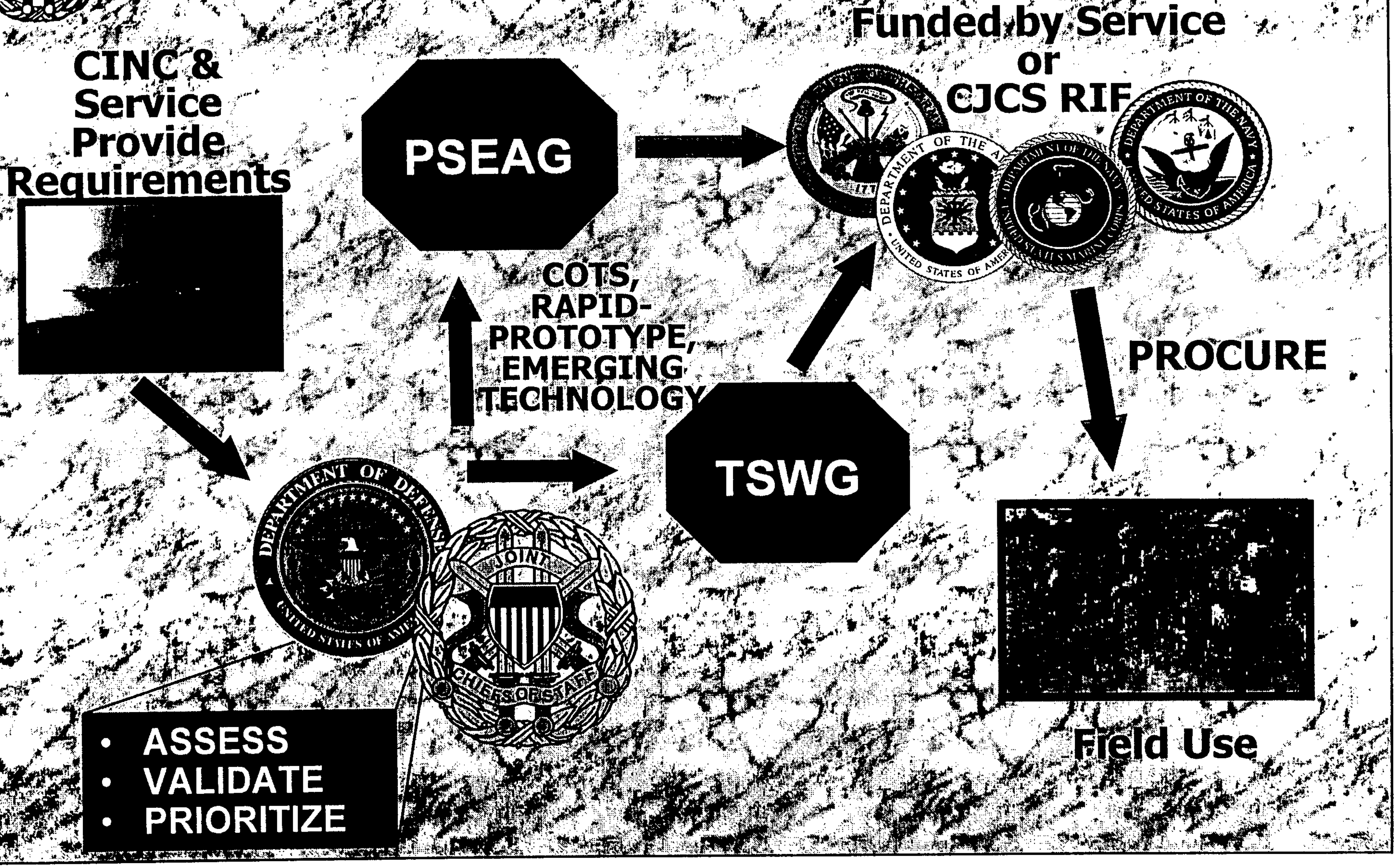
FORCE PROTECTION SESSION

Michael Toscano - Chairman

Fourteenth Annual NDIA Security Symposium and Exhibition

June 17, 1998

Technology Process



CINC & Service Provide Requirements

PSEAG

COTS, RAPID-PROTOTYPE, EMERGING TECHNOLOGY

TSWG

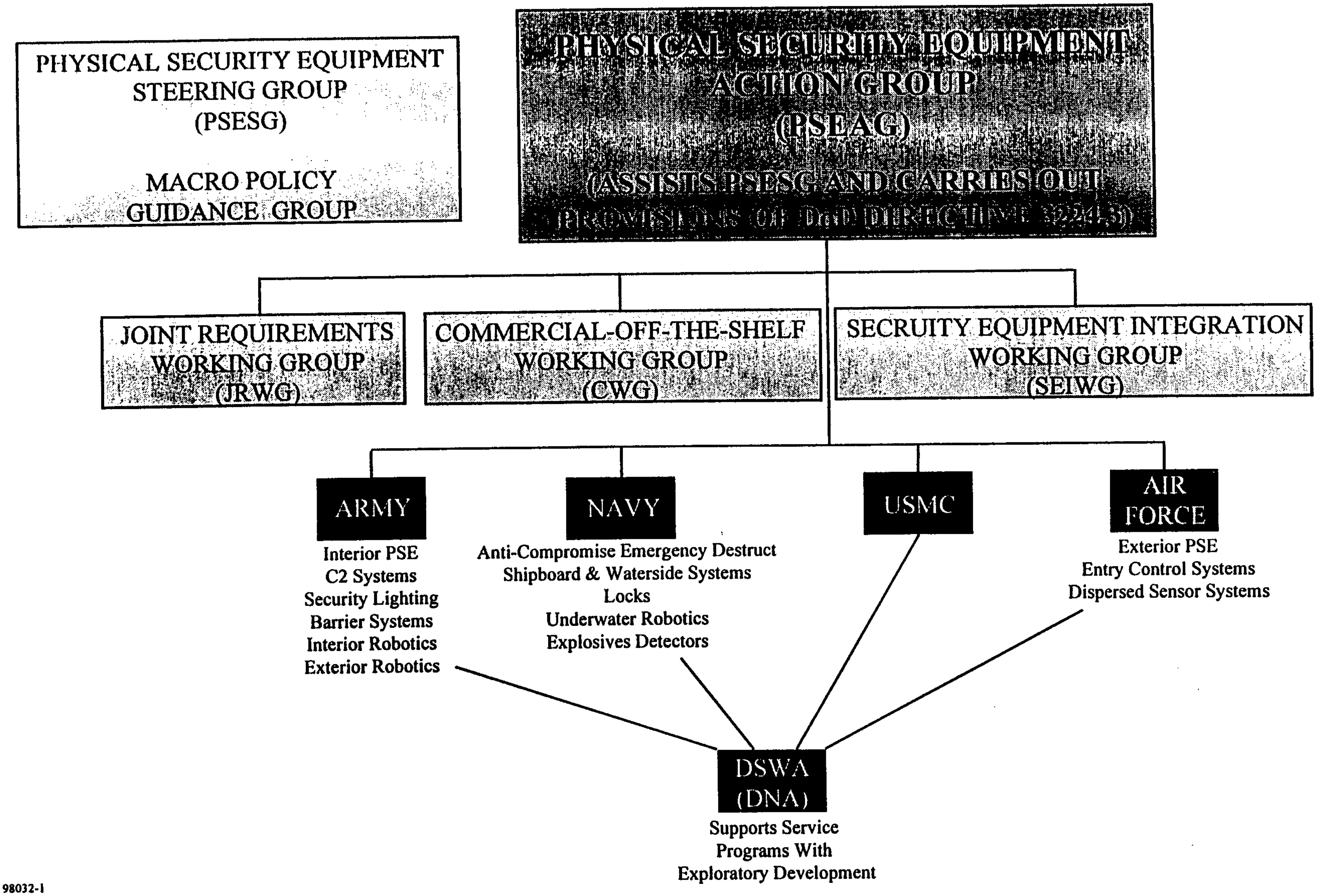
Funded by Service or CJCS RIF

PROCURE

Field Use

- ASSESS
- VALIDATE
- PRIORITIZE

Physical Security Equipment Action Group (PSEAG)



PHYSICAL SECURITY EQUIPMENT STEERING GROUP (PSESG)

MACRO POLICY GUIDANCE GROUP

PHYSICAL SECURITY EQUIPMENT ACTION GROUP (PSEAG)

(ASSISTS PSESG AND CARRIES OUT PROVISIONS OF DoD DIRECTIVE 3224.3)

JOINT REQUIREMENTS WORKING GROUP (JRWG)

COMMERCIAL-OFF-THE-SHELF WORKING GROUP (CWG)

SECRUITY EQUIPMENT INTEGRATION WORKING GROUP (SEIWG)

ARMY

Interior PSE
C2 Systems
Security Lighting
Barrier Systems
Interior Robotics
Exterior Robotics

NAVY

Anti-Compromise Emergency Destruct
Shipboard & Waterside Systems
Locks
Underwater Robotics
Explosives Detectors

USMC

AIR FORCE

Exterior PSE
Entry Control Systems
Dispersed Sensor Systems

DSWA (DNA)

Supports Service
Programs With
Exploratory Development

NDIA Security Technology Symposium

Wednesday 17 June 1998

<u>10:00 am SESSION V (a)</u> DoD FORCE PROTECTION

This session will address the Services' initiatives, organizational changes and technology focus areas being conducted through the DoD Physical Security Equipment Action Group (PSEAG), in their continuing efforts to combat terrorism and provide force protection.

Session Introduction:
Mr. Michael Toscano, Chairman,
DoD Physical Security Equipment Action
Group (PSEAG), OUSD (A&T)
Washington, DC

10:15 – 10:40
Featured Speaker
Brigadier General James Conway, USMC
Deputy Director of Combating Terrorism
Joint Chiefs of Staff - J-34
Washington, DC

10:45 am
DoD PSEAG Program Presentations:

ARMY
10:45-11:00
LTC Bruce Swagler
CECOM, PM-PSE
Ft. Belvoir, VA

AIR FORCE
11:00-11:15
Col Russell Peter
HQ ESC/FD
Hanscom AFB, MA

NAVY
11:15-11:30
Ms. Shirley Mattingly,
ESS Program Manager
Navy Criminal Investigative Service
Washington, DC

11:30 LUNCH

NDIA Security Technology Symposium

12:30 pm SESSION V (b) DoD FORCE PROTECTION

DSWA
12:30-12:45

Mr. William J. Witter
Chief, Physical Security
Defense Special Weapons Agency
Alexandria, VA

DPS
12:45-1:00

Mr. John Jester
Chief, Defense Protective Service
The Pentagon
Washington, DC

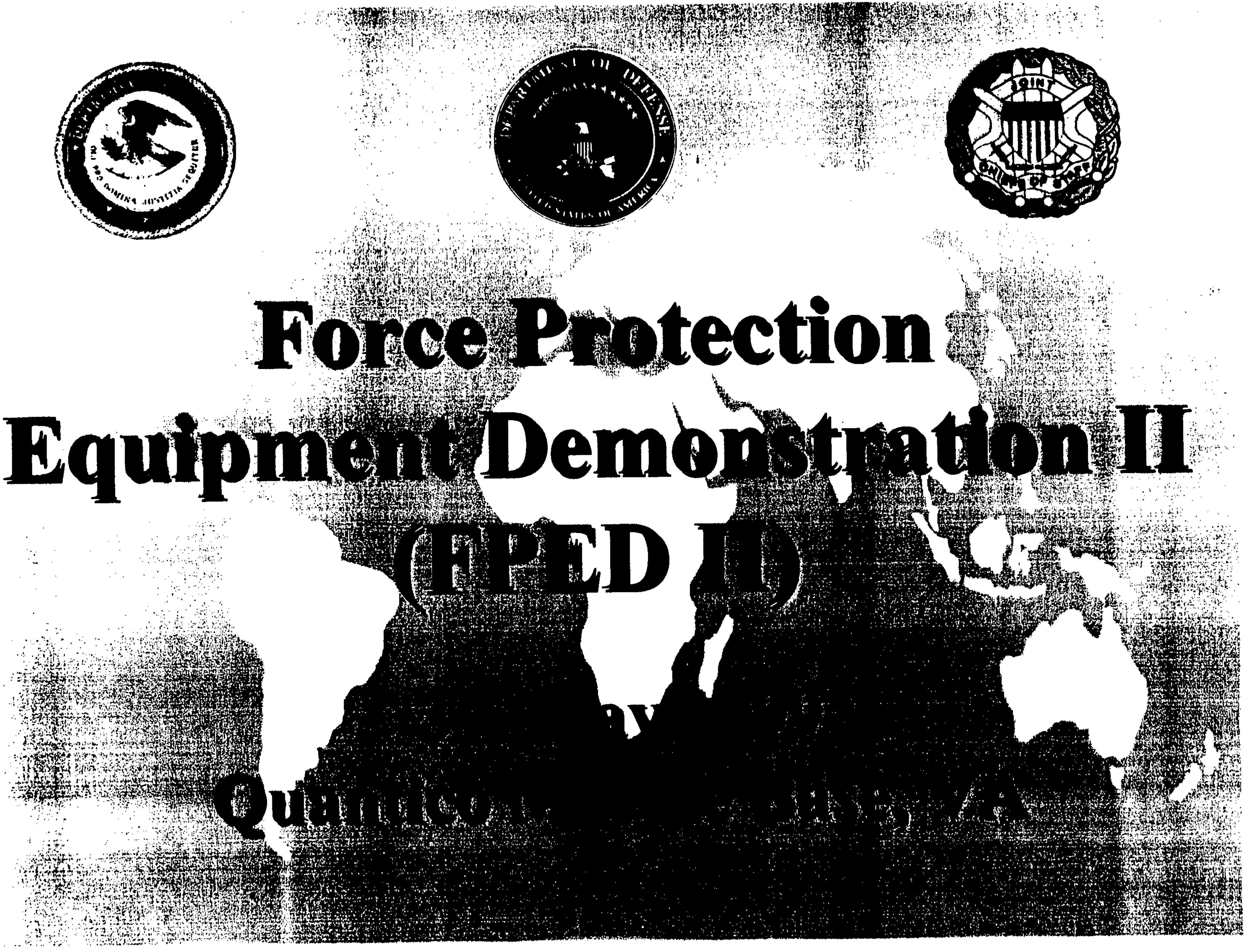
1:00 - 1:30 pm DoD Panel Question & Answer Session/Wrap-Up To Include:

• Mr. Mike Toscano	OUSD	• Col Russ Peter	AF/ESC
• BG James Conway	J-34	• Col Don Collins	Battlelab
• LTC Bruce Swagler	Army	• Mr. Leo Targosz	Navy
• Mr. Jerry Edwards	Army	• Mr. Jeff Edwards	USMC
• Mr. John Jester	DPS	• Mr. Bill Witter	DSWA

Force Protection Equipment Demonstration II Update - (4 min. video)

Closing Remarks

1:30 pm Session VII: Transportation Security

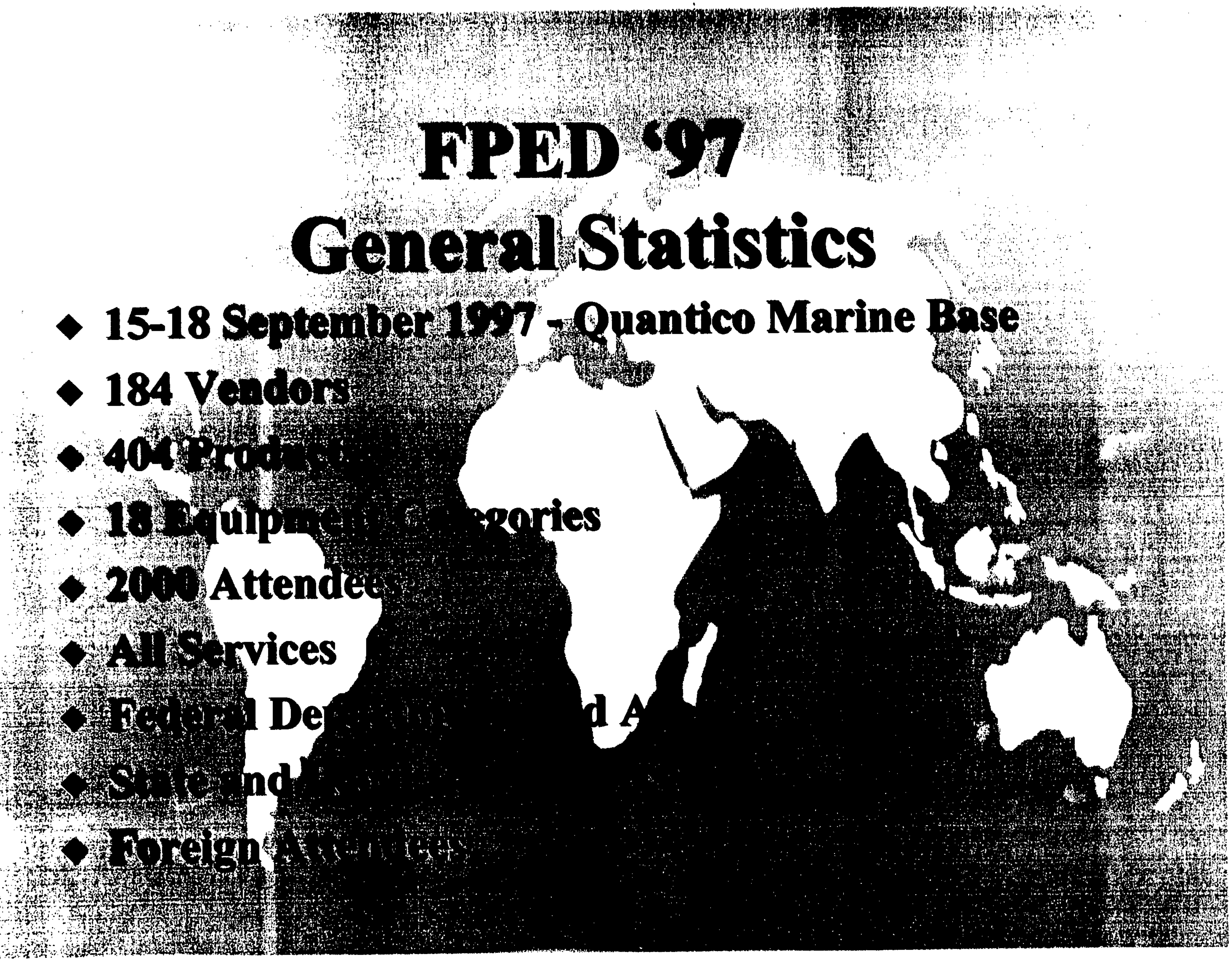


Force Protection Equipment Demonstration II (FPED II)

[illegible]ay [illegible]

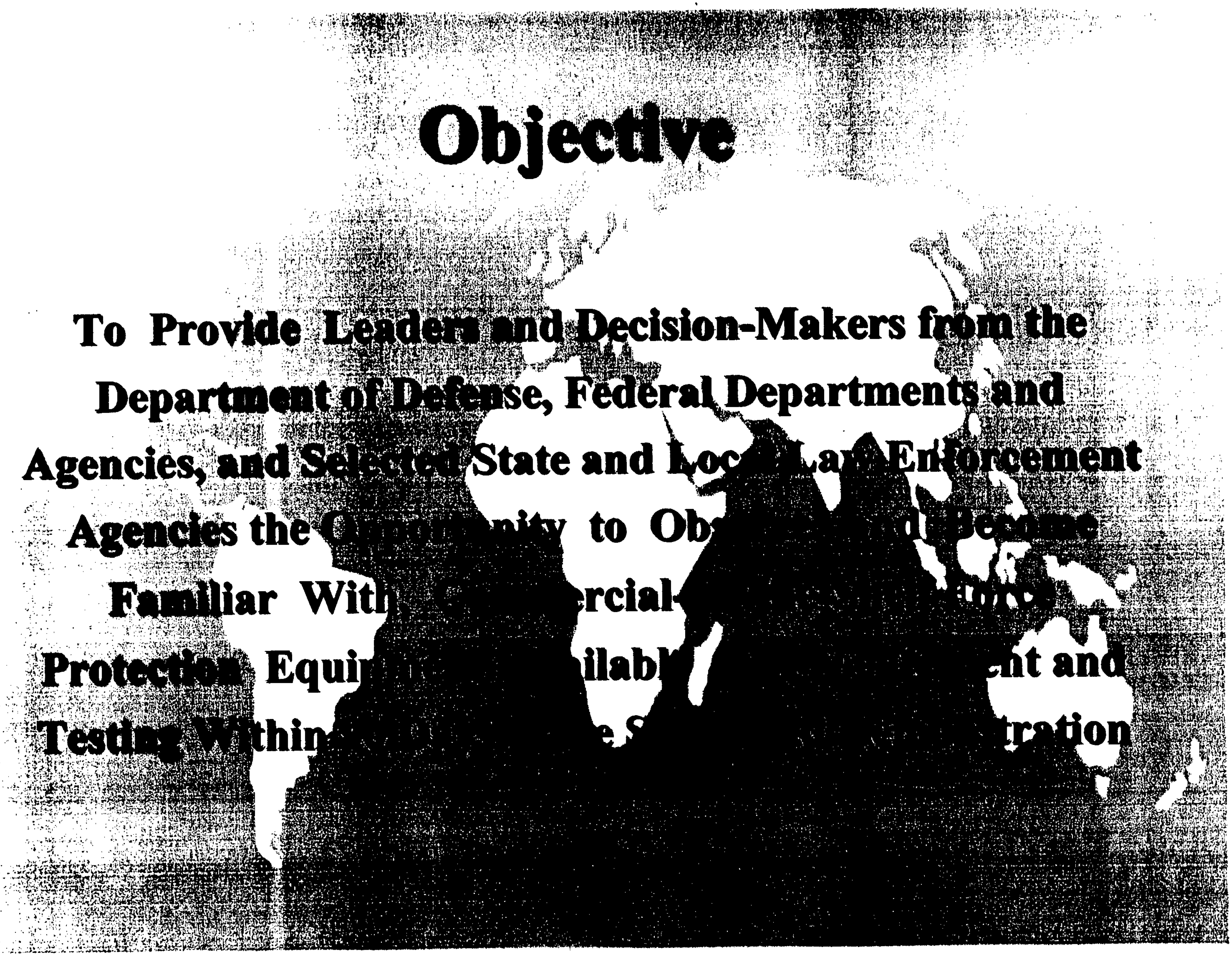
Quantico [illegible], VA

FPED '97
General Statistics

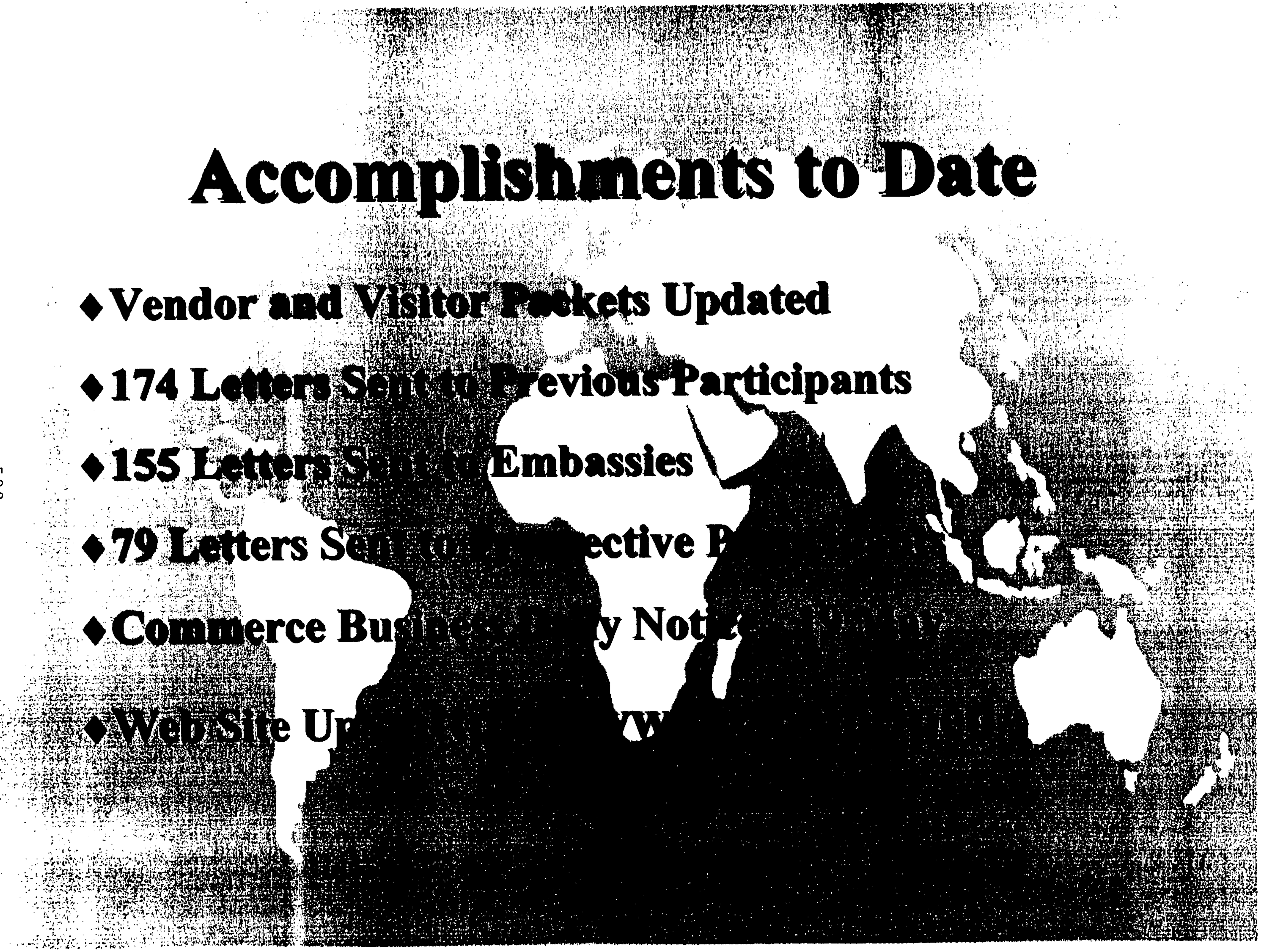


- 15-18 September 1997 - Quantico Marine Base
- 184 Vendors
- 404 Products
- 18 Equipment Categories
- 2000 Attendees
- All Services
- Federal Departments and A[illegible]
- State and [illegible]
- Foreign Attendees

Objective

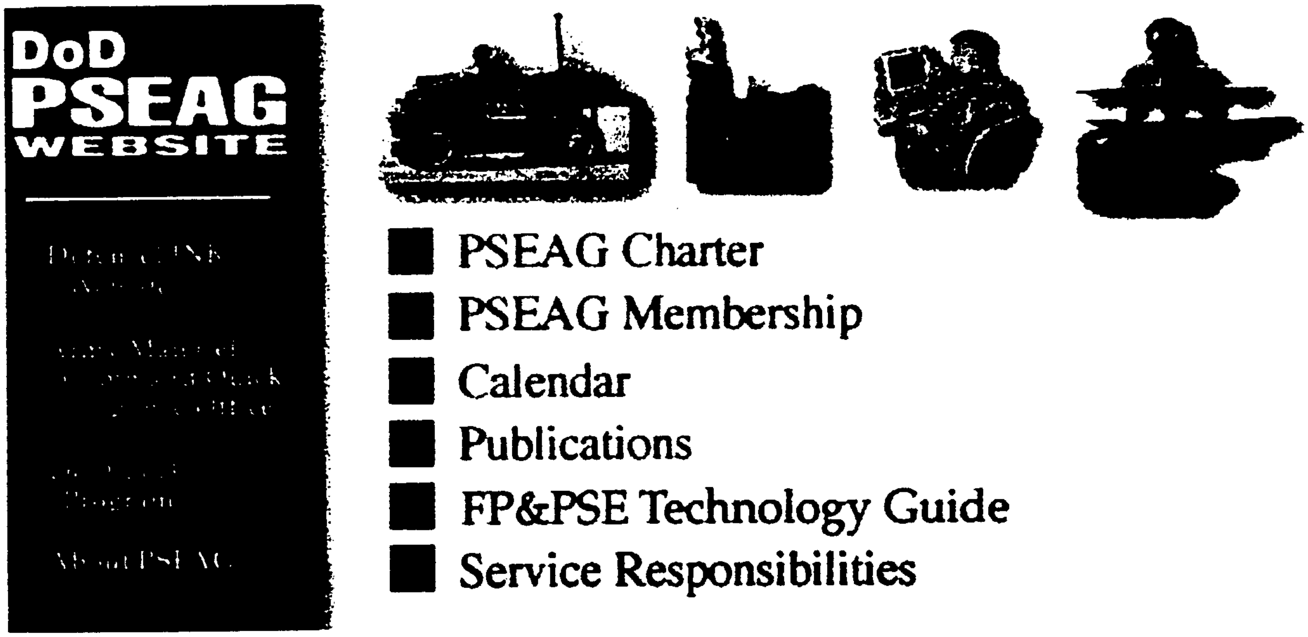


To Provide Leaders and Decision-Makers from the Department of Defense, Federal Departments and Agencies, and Selected State and Local Law Enforcement Agencies the Opportunity to Ob[illegible] and Become Familiar With [illegible]ercial-[illegible] Force Protection Equip[illegible] [illegible]ilabl[illegible] [illegible]nt and Testing Within [illegible] [illegible]e S[illegible] [illegible]tration



Accomplishments to Date

- ♦ Vendor and Visitor Packets Updated
- ♦ 174 Letters Sent to Previous Participants
- ♦ 155 Letters Sent to Embassies
- ♦ 79 Letters Sent to Prospective B[illegible]
- ♦ Commerce Business Daily Notice [illegible]
- ♦ Web Site U[illegible] WWW[illegible]



DoD
PSEAG
WEBSITE

[illegible]

[illegible]

[illegible] Program

About PSEAG

- PSEAG Charter
- PSEAG Membership
- Calendar
- Publications
- FP&PSE Technology Guide
- Service Responsibilities

For Further PSEAG Information contact our Web Site at: http://www.csc.com/pseag/index.html

Point of Contact

OUSD A&T (S&TS/LW)
ATTN: Mr. Michael Toscano
Pentagon, Room 3B1060
Washington, DC 20301

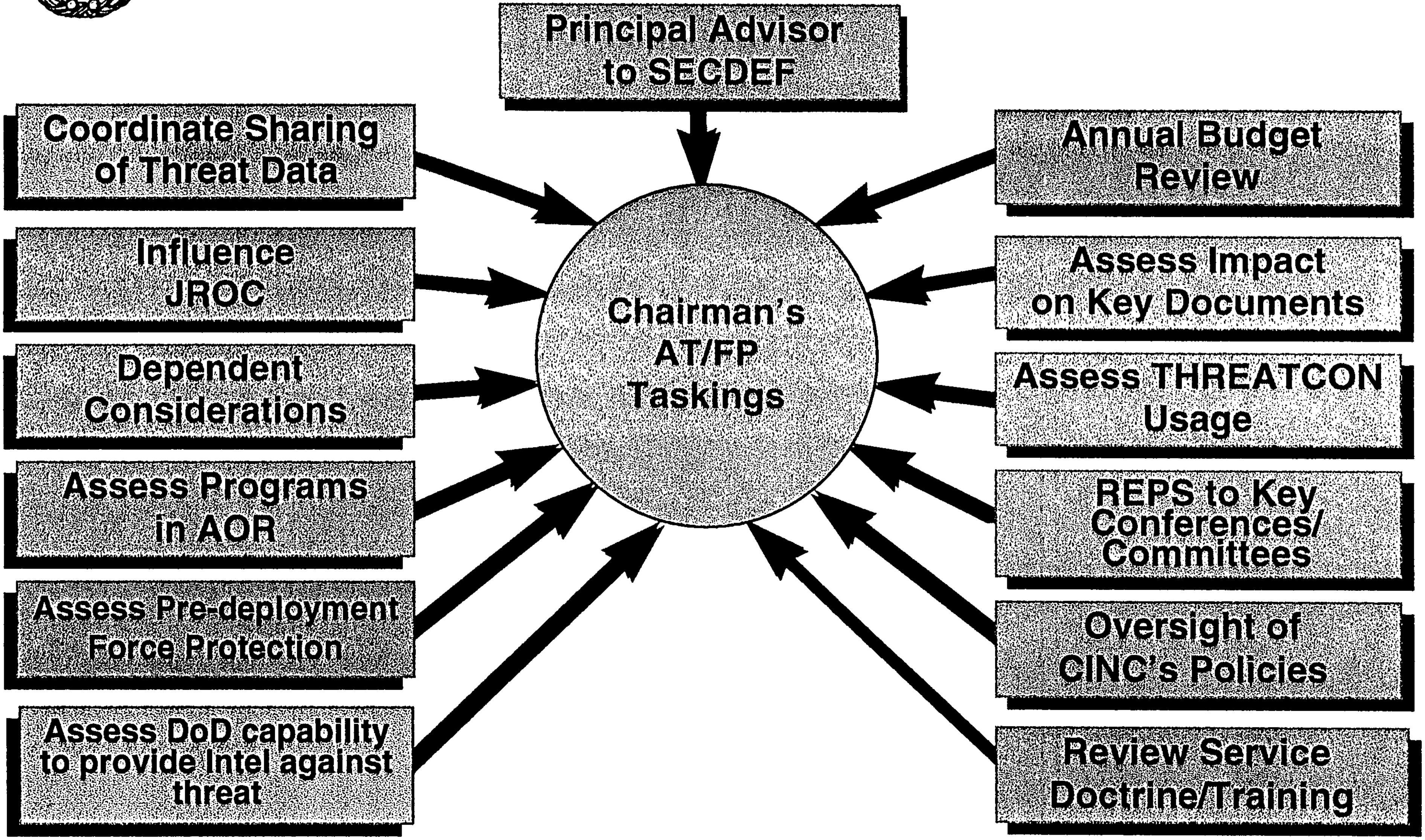
Phone: (703) 697-0638
DSN: 227-0638
Fax: (703) 693-7029
E-Mail: toscanom@acq.osd.mil

Combating Terrorism

BGen Conway
Joint Staff/J-34

NDIA
17 June 1998

Chairman's Tasks



Principal Advisor to SECDEF

Chairman's AT/FP Taskings

Coordinate Sharing of Threat Data

Influence JROC

Dependent Considerations

Assess Programs in AOR

Assess Pre-deployment Force Protection

Assess DoD capability to provide Intel against threat

Annual Budget Review

Assess Impact on Key Documents

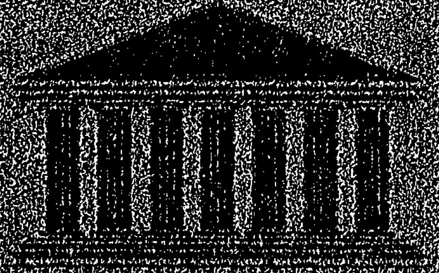
Assess THREATCON Usage

REPS to Key Conferences/ Committees

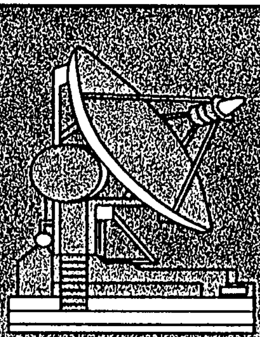
Oversight of CINC's Policies

Review Service Doctrine/Training

Areas of Emphasis

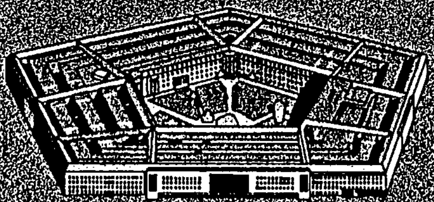


EDUCATION, TRAINING, AND DOCTRINE

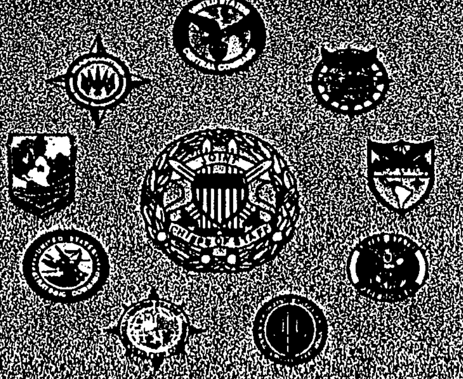


RESOURCES AND TECHNOLOGY

STANDARDS AND ASSESSMENTS

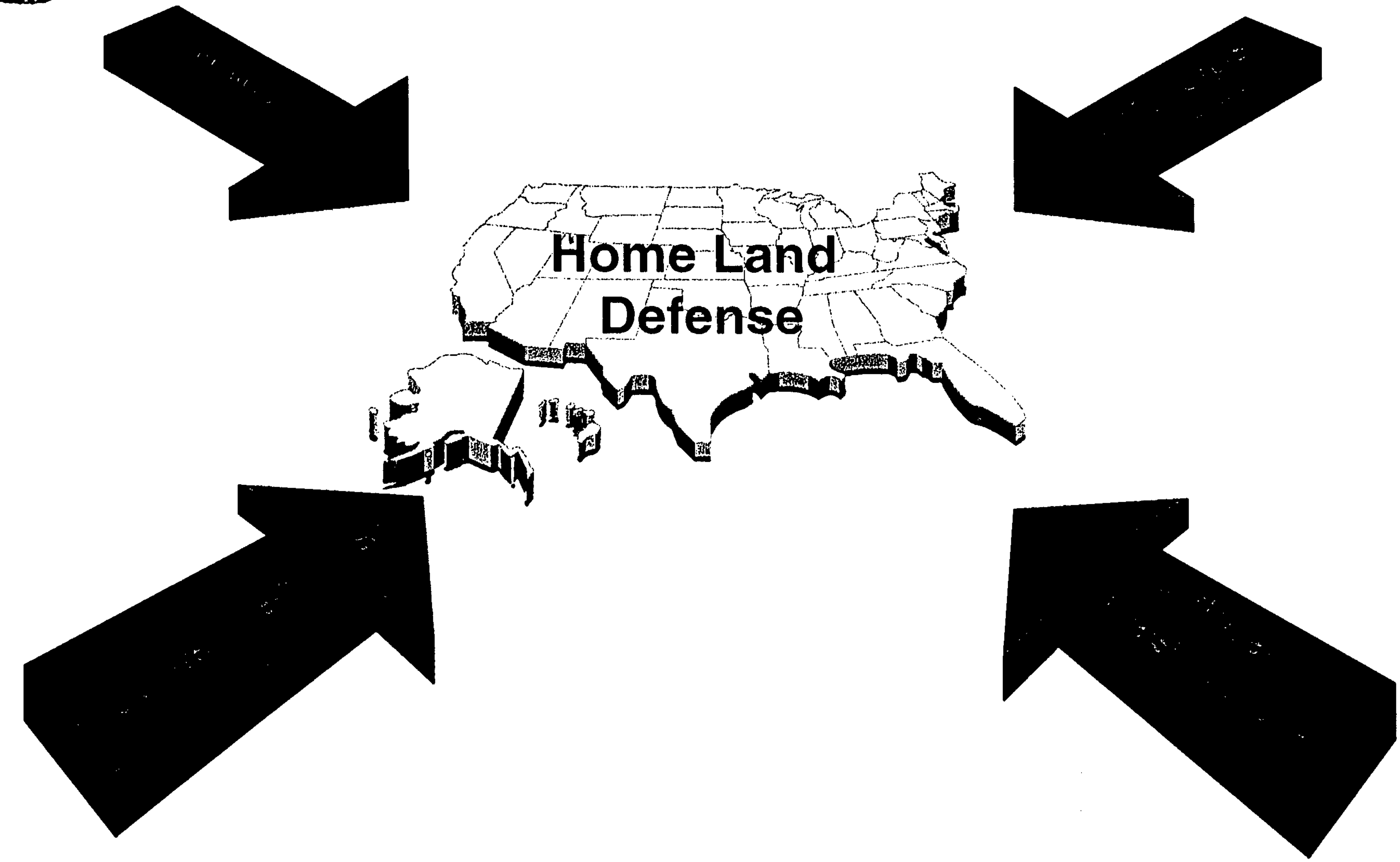


POLICY COORDINATION



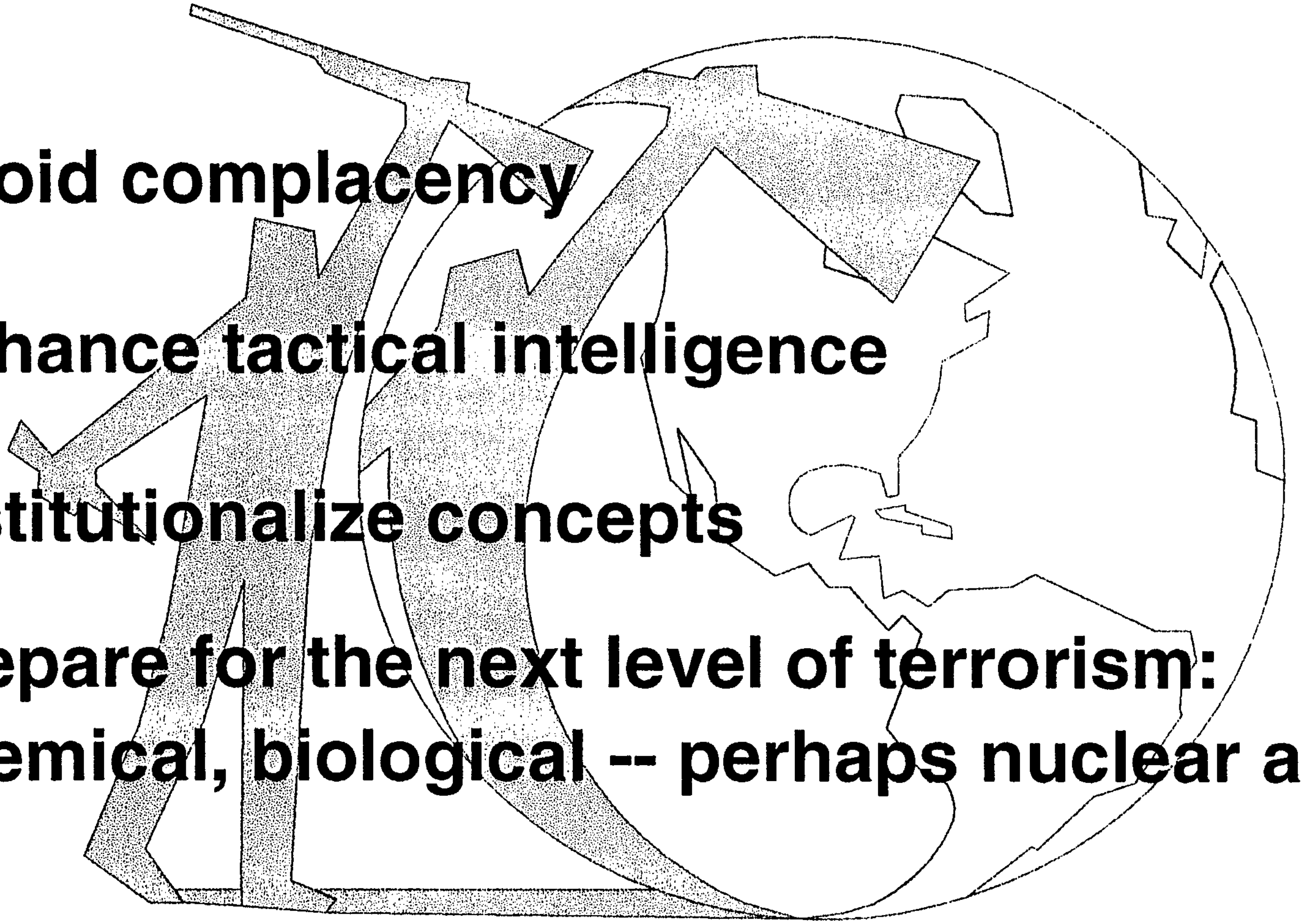
OPERATIONAL FUSION

The Current Thrust



Home Land
Defense

Challenges



- Avoid complacency
- Enhance tactical intelligence
- Institutionalize concepts
- Prepare for the next level of terrorism: chemical, biological -- perhaps nuclear attack

JCS Subject Areas for COTS Testing

1. Personnel Alerting Systems
2. Explosive Detection Devices
3. Explosive Mitigation
4. Personal Protection Equipment
5. Ground Sensors
6. Active Barriers
7. Passive Barriers
8. Thermal Imaging Devices
9. Wide Area Security & Surveillance System
10. Under vehicle surveillance Systems

U.S. Army Communications-Electronics Command

PM-PSE

Product Manager, Physical Security Equipment

LTC Bruce M. Swagler, Product Manager
DSN: 654-2416/COMM: (703) 704-2416
E-MAIL: bswagler@belvoir.army.mil

PM-PSE Mission

PM-PSE

Product Manager, Physical Security Equipment

Provide cost-effective, state-of-the-art and logistically supportable physical security systems to installations and forces deployed worldwide

Army Executive Agent For PSE Army Materiel Command

PM-PSE

Product Manager, Physical Security Equipment

- Has been delegated authority by AAE to administer Army RDA PSE programs IAW established policies and procedures
- Single point of contact for all PSE
  - Conventional - Nuclear - Chemical
- Central manager for planning, acquisition, development, installation and support of PSE
- Other tasks
  - Implement DoD Dir 3224.3
  - Appoint Army rep to DoD Physical Security Equipment Action Group (PSEAG)
  - Represent Army on DoD Physical Security Equipment Steering Group (PSESG)
  - Appoint chair to the DA PSEAG

System Development & Fielding Philosophy

PM-PSE

Product Manager, Physical Security Equipment

- Maximize use of Commercial Off The Shelf (COTS) products
- Phased approach to fielding
- Early fielding of cost-effective equipment to the user
- Maintain a Pre-Programmed Product Improvement (P^3I) program to provide better or enhanced capability against the threat

DoD Directive

- Congress directed management responsibility with OSD (A) TS/LS
- All PSE R&D funding consolidated into a single program element
- Joint Service coordination and OSD oversight management accomplished through Physical Security Equipment Action Group (PSEAG)
- Services responsible for management of procurement and installation effort
- DSWA assigned responsibility to support all Services 6.2 efforts
- Directs centralized management of Services RDT&E efforts at DoD level
- Directs each Service to establish a single POC for PSE
- Directs each Service to establish a PSE Program Management Office
- Assigns specific functional areas of responsibility to each Service for RDT&E

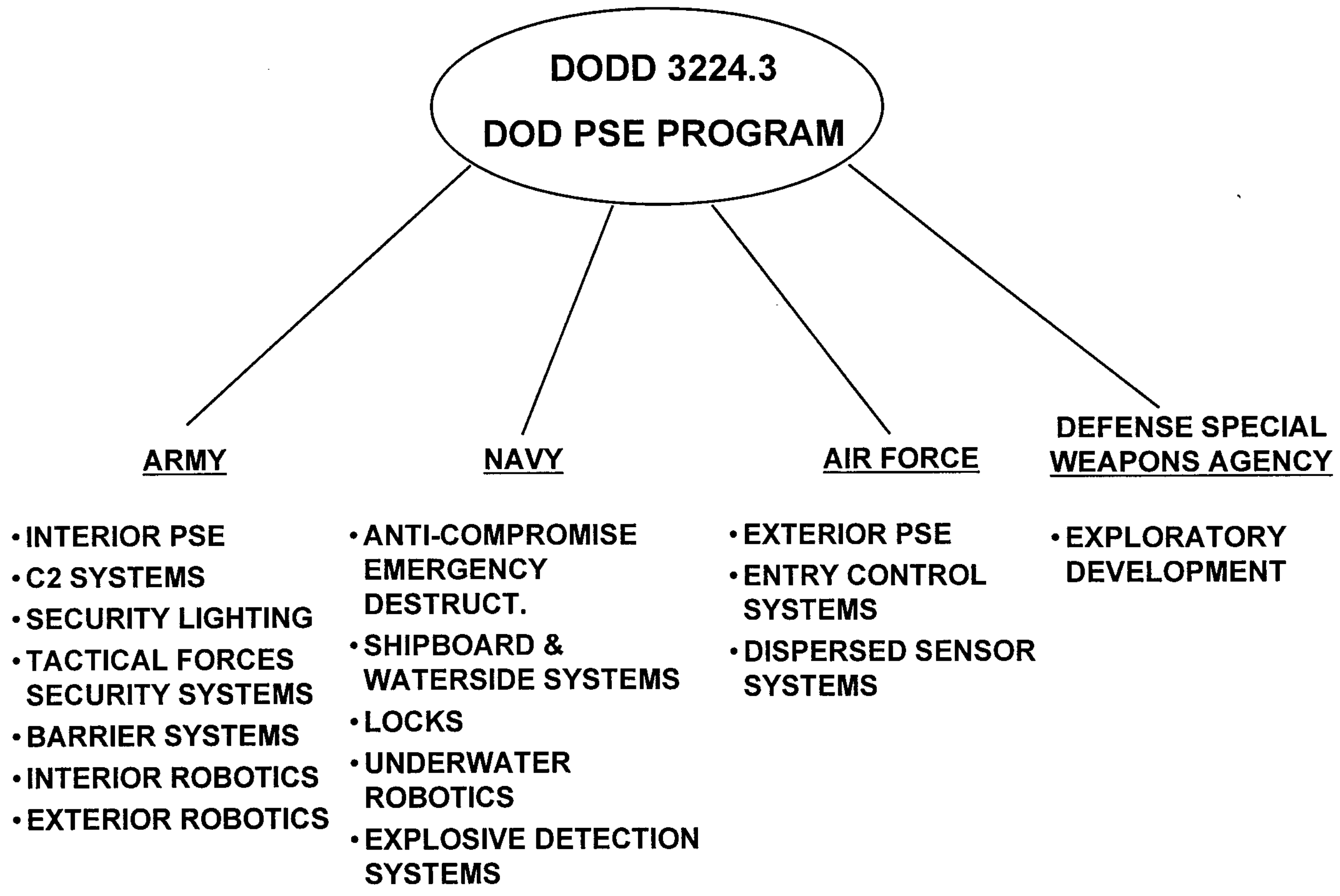
US ARMY CECOM SYSTEMS MANAGEMENT CENTER

SMC

Responsibilities

PM-PSE

Product Manager, Physical Security Equipment



DODD 3224.3

DOD PSE PROGRAM

ARMY

- INTERIOR PSE
- C2 SYSTEMS
- SECURITY LIGHTING
- TACTICAL FORCES SECURITY SYSTEMS
- BARRIER SYSTEMS
- INTERIOR ROBOTICS
- EXTERIOR ROBOTICS

NAVY

- ANTI-COMPROMISE EMERGENCY DESTRUCT.
- SHIPBOARD & WATERSIDE SYSTEMS
- LOCKS
- UNDERWATER ROBOTICS
- EXPLOSIVE DETECTION SYSTEMS

AIR FORCE

- EXTERIOR PSE
- ENTRY CONTROL SYSTEMS
- DISPERSED SENSOR SYSTEMS

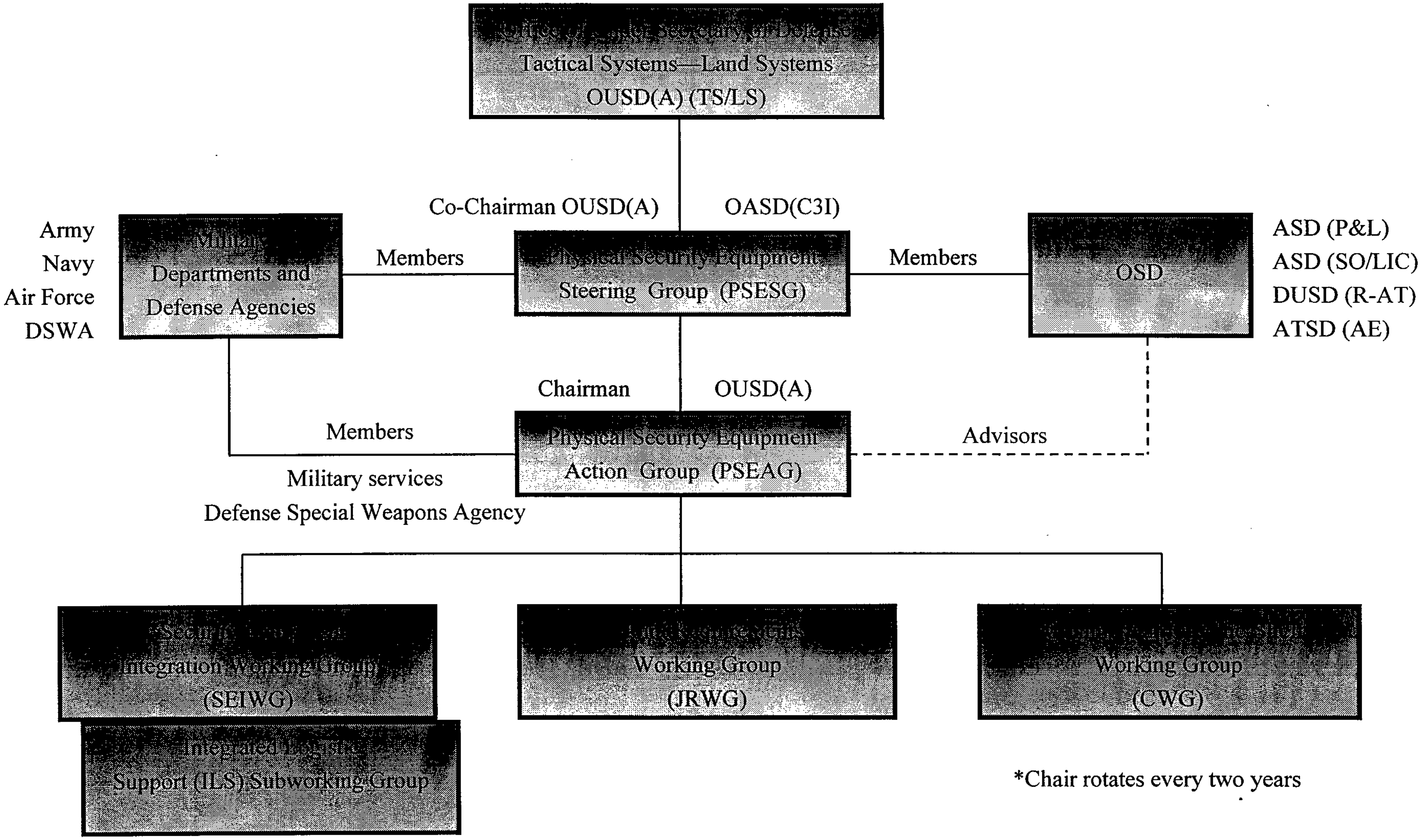
DEFENSE SPECIAL WEAPONS AGENCY

- EXPLORATORY DEVELOPMENT

US ARMY CECOM SMC SYSTEMS MANAGEMENT CENTER

DoD Physical Security Equipment Programs — Advisory Management Organizations

PM-PSE
Product Manager, Physical Security Equipment

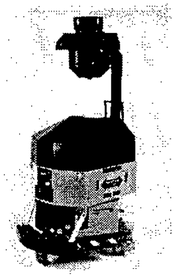

Office of [illegible] Secretary of Defense
Tactical Systems—Land Systems
OUSD(A) (TS/LS)
Co-Chairman OUSD(A)
OASD(C3I)
Army
Navy
Air Force
DSWA
Military Departments and Defense Agencies
Members
Physical Security Equipment Steering Group (PSESG)
Members
OSD
ASD (P&L)
ASD (SO/LIC)
DUSD (R-AT)
ATSD (AE)
Chairman
OUSD(A)
Members
Physical Security Equipment Action Group (PSEAG)
Advisors
Military services
Defense Special Weapons Agency
Securi[illegible]
Integration Working Group
(SEIWG)
Integrated Logistic
Support (ILS) Subworking Group
[illegible] Requirements
Working Group
(JRWG)
[illegible]
Working Group
(CWG)

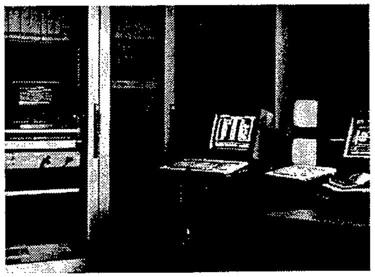
*Chair rotates every two years

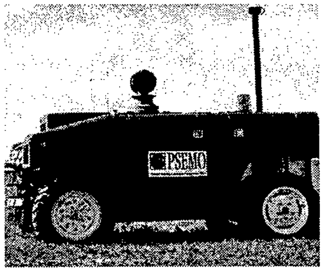
ADVANCED SENSORS

SUPPORTING MAJOR PROGRAM TITLE: INTRUSION DETECTION SYSTEM

Advanced Sensor Upgrades







DESCRIPTION/OBJECTIVE

Advanced Sensors (AS) Investigate New and Emerging Sensor Technology for Application to ICIDS, MDARS and MSSMP. Once Technically Mature, the Sensors will be Fielded in Integrated Groups (I,II) over the entire Program Life Cycle. Technologies Include Fiber Optics, Wireless Sensors, Presence Sensors and Electronic Article Surveillance. Sensor Projects Transitioned from DSWA will be Developed under this Program. These Sensors will provide the Advanced Capability of Detecting/Determining Unauthorized Entry or Attempted Intrusions into Facilities by an Increasingly Sophisticated Threat.

SIGNIFICANT ACCOMPLISHMENTS - FY97

- Prepared and Submitted 6.2 PSE Research Proposals
- Monitored TASS Technology Development & Capabilities
- Established TSE Testbed
- Conducted TSE System Evaluations
- Supported TSE Requirement Definition
- Monitored/Evaluated PSE Technologies for ICIDS Technology Insertion
- Conducted PSE and TSE Market Surveillance

AGENCY: U.S. Army
POINT OF CONTACT: Product Manager,
Physical Security Equipment
PHONE NUMBER: (703) 704-2416

PROJECTED ACCOMPLISHMENTS

FY98

- Conduct PSE and TSE Technology Market Surveillance
- Support ETF Market Investigation
- Evaluate Candidate COTS Sensors

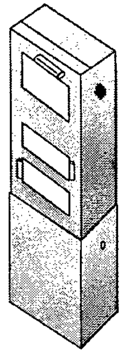
FY99

- Conduct PSE and TSE Technology Market Surveillance
- Evaluate Candidate COTS Sensors

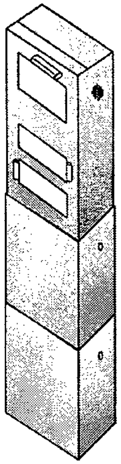
5/19/98

ELECTRONIC TRIP FLARE (ETF)

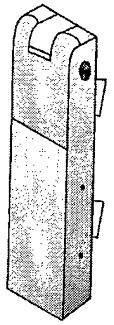
SUPPORTING MAJOR PROGRAM TITLE: TACTICAL SECURITY EQUIPMENT



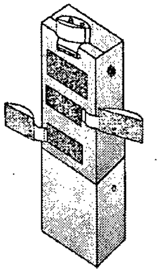
• BASIC ETF



• ETF W/ONE EXTRA BATT



• ETF CARRYING & MOUNTING CASE



• ETF DEPLOYED

DESCRIPTION/OBJECTIVE

ETF will be a lightweight, manportable, easily emplaced and recoverable motion activated device designed to provide early warning and illumination to individuals and small units. This capability will provide commanders with an increase in time to effectively determine the most appropriate tactical response. The ETF will be used as an independent/ individually employed early warning device or as a part of a security concept layer.

SIGNIFICANT ACCOMPLISHMENTS - FY97

- Completed Operational Requirements Document (ORD) Worldwide Staffing
- ORD approved by TRADOC on 29 May 97
- PM-PSE assigned as Materiel Developer
- Completed Milestone 0

AGENCY: U.S. Army
POINT OF CONTACT: Product Manager,
Physical Security Equipment
PHONE NUMBER: (703) 704-2416

PROJECTED ACCOMPLISHMENTS

FY98

- Awaiting allocation of PSEAG Funding
- Conduct MS/MI

FY99

- Develop Tailored Concept Formulation Package

5/19/98

FORCE PROTECTION EQUIPMENT DEMONSTRATION-II (FPED-II)

SUPPORTING MAJOR PROGRAM TITLE: PROGRAM MANAGEMENT

DESCRIPTION/OBJECTIVE

The purpose of the demonstration is to provide a first-hand look at Commercial-off-the-Shelf force protection equipment that is immediately available for procurement to military commanders and Department of Defense (DoD) decision-makers. Those items of equipment which appear, on the basis of the demonstration, to meet needs within the DoD will be prioritized for possible follow-on testing and procurement beginning in FY00. Any procurement of equipment will be made by the Military Services.

SIGNIFICANT ACCOMPLISHMENTS - FY98

• Executive Coordination Committee and Project Officer's Group Formed	4/30/98
• 177 Invitations Mailed to Previous Vendors	4/30/98
• Web Site Activated (http://www.csc.com/fped)	5/1/98
• Invitations Mailed to 155 Embassies	5/6/98
• 68 Invitations Mailed to Prospective Vendors	5/12/98
• Conducted Initial Discussions with Support Contractors	5/13/98
• Commerce Business Daily Notice Published	5/19/98
• J34 PAO Planning Meeting Conducted	5/19/98

AGENCY: U.S. Army
POINT OF CONTACT: Product Manager,
Physical Security Equipment
PHONE NUMBER: (703) 704-2416

PROJECTED ACCOMPLISHMENTS

FY98

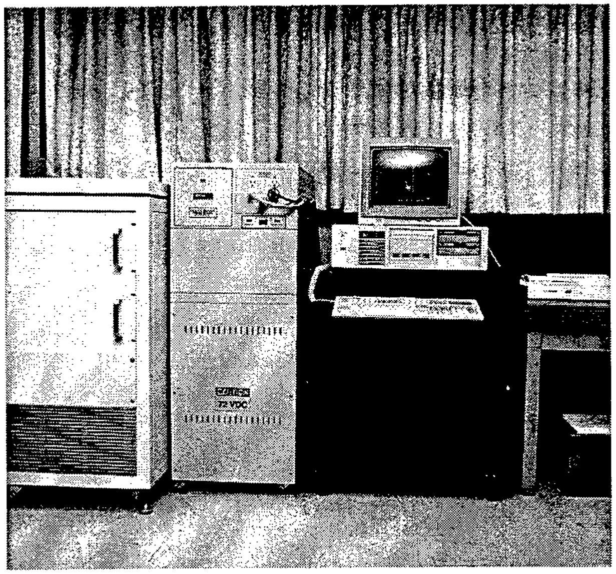
- Mail invitations to Prospective Vendors
- Conduct Publicity to Attract Vendors
- Request Additional Facilities at Quantico
- Conduct Vendor Site Visit - August 27
- Accept Applications from Vendors

FY99

- Send Acceptance Letters/LOIs to Vendors
- Conduct Detailed Planning of Demonstrations and finalize site layout
- Publicize FPED II to Attract Attendees
- Finalize MOA and LOI with Quantico
- Send LOIs to Attendees
- Set-up and Conduct FPED II

5/19/98

ALARM MONITOR GROUP
(AMG)
SUPPORTING MAJOR PROGRAM TITLE: INTRUSION DETECTION SYSTEM



DESCRIPTION/OBJECTIVE

Alarm Monitor Group (AMG) is a Materiel Change (MC) to the Joint-Services Interior Intrusion Detection System. The current configuration indicates system status changes (alarm/no-alarm, access/secure, and AC/battery power) by flashing lights and audio beeper. Using a personal computer based upgrade, the MC provides graphics display of status changes according to user-assigned priorities. Additional capabilities include automatic resynchronization and system summary display.

SIGNIFICANT ACCOMPLISHMENTS - FY97

- Installed 4 Systems in CONUS
- Installed 4 Systems Hawaii
- Installed 4 Systems Europe

AGENCY: U.S. Army
POINT OF CONTACT: Product Manager,
Physical Security Equipment
PHONE NUMBER: (703) 704-2416

PROJECTED ACCOMPLISHMENTS
FY98

- Install 3 Systems Korea
- Install 4 Systems Europe
- Install 2 System CONUS
- Total Systems Installed to Date: 66

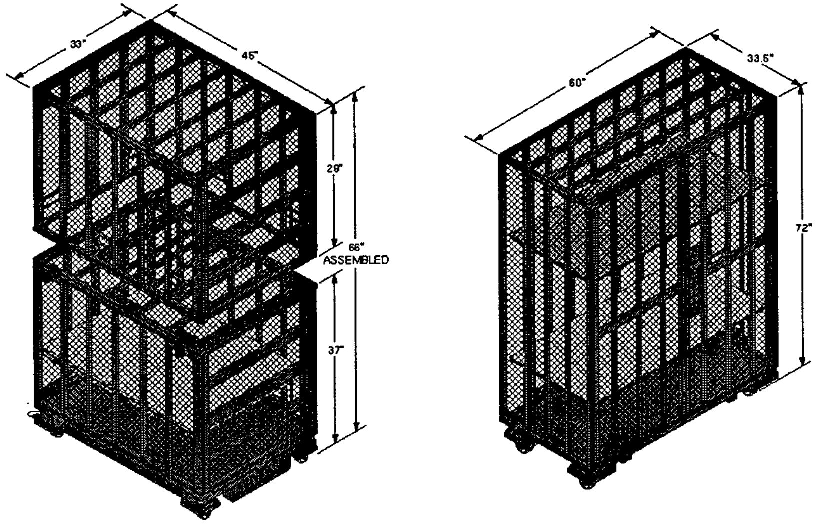
FY99

- Install 1 System Korea
- Install 4 Systems Europe
- Install 1 Systems Southwest Asia

HIGH-VALUE ASSET SECURITY CONTAINER (HVASC)

Phase I (Security Container)

SUPPORTING MAJOR PROGRAM TITLE: HIGH VALUE ITEM SECURITY SYSTEM (HVISS)



DESCRIPTION/OBJECTIVE

The HVASC will provide Commanders a container to secure high-value items in both Garrison and Field Environments. The HVASC will increase readiness and sustainability by ensuring the unit maintains on-hand equipment accountability of highly pilferable, sensitive items such as Night Vision Devices (NVDs), global positioning devices, etc. The HVASC will be applicable for currently fielded systems and high technology items soon to be fielded.

SIGNIFICANT ACCOMPLISHMENTS - FY97

- Finalized Commercial Drawing Package
- Completed Army Distribution List
- Completed Army Directed Procurement Package
- Completed Safety Release Testing (ATC 18 Aug-2 Sep)
- Completed Safety Assessment Report

AGENCY: U.S. Army
POINT OF CONTACT: Product Manager,
Physical Security Equipment
PHONE NUMBER: (703) 704-2416

PROJECTED ACCOMPLISHMENTS
FY98

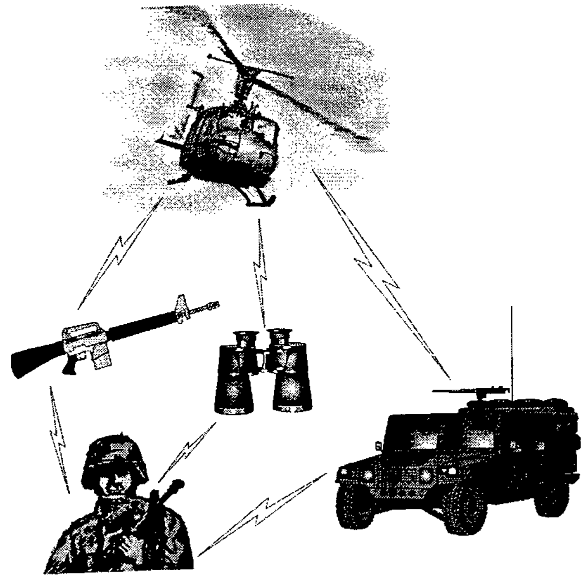
- Complete Logistic Support Package
- Complete Increase to Direct Procurement Package for 1,000 HVASC
- Award Procurement Contract

FY99

- Complete Production of HVASC's as required

5/19/98

HIGH-VALUE ITEM SECURITY SYSTEM (HVISS)
Phase II (RFID)
SUPPORTING MAJOR PROGRAM TITLE: HIGH VALUE ITEM SECURITY SYSTEM (HVISS)



DESCRIPTION/OBJECTIVE

The HVISS Phase II will provide Commanders a system to locate and recover high value items in both garrison and field environments. The HVISS will increase readiness and sustainability by ensuring the unit maintains on-hand equipment accountability of highly pilferable, sensitive items such as Night Vision Devices (NVDs) and global positioning devices, etc. The HVISS Phase II will be applicable for other High Value, High Technology Items now fielded or soon to be fielded.

SIGNIFICANT ACCOMPLISHMENTS - FY97

- Completed initial staffing of Operational Requirements Document (ORD)
- Completed Trade-Off Analysis (Approved July 97)
- Initiated miniaturized Radio Frequency Identification (RFID) Tagging/Tracking Applied Research (6.2) Prioritization

AGENCY: U.S. Army
POINT OF CONTACT: Product Manager,
Physical Security Equipment
PHONE NUMBER: (703) 704-2416

PROJECTED ACCOMPLISHMENTS
FY98

- Continue ORD staffing for Milestone I
- Transition to Milestone I
- Prepare RFID BAA
- Continue Miniaturized RF Tagging/Tracking 6.2 Effort

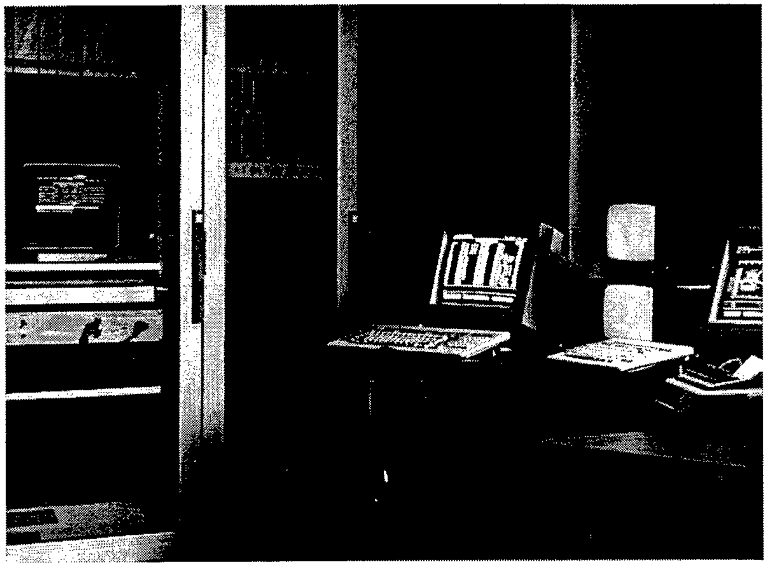
FY99

- Finalize ORD for Milestone I
- Prepare the BTA
- Award RFID BAA Contract
- Transition Miniaturized RF Tagging/Tracking 6.2 Effort

5/19/98

INTEGRATED COMMERCIAL INTRUSION DETECTION SYSTEM (ICIDS)

SUPPORTING MAJOR PROGRAM TITLE: INTRUSION DETECTION SYSTEM



DESCRIPTION/OBJECTIVE

The ICIDS is a program pursuing a nondevelopmental item acquisition approach providing a joint service system protecting high dollar and critical defense and other government assets. The ICIDS is a highly secure standardized intrusion detection system using state-of-the-art technology. This program replaces aging and obsolete equipment and upgrades installation security to required levels without an increase in manpower.

SIGNIFICANT ACCOMPLISHMENTS - FY97

- Installations in Progress at Fort Polk, Ft. Campbell, and FBI Hoover Building
- Awarded ICIDS II Contract
- Issued ICIDS II Delivery Order for Ft. Bliss
- Conducted Site Design of ICIDS I at Vicenza, Italy
- Complete Installation at FBI Hoover Building
- Provide ICIDS I Support to Whitemen AFB, Ft. Bragg, Ft. Carson, Ft. Sill, Ft. Rucker, and Ft. Gordon
- Issue Delivery Order for Capitol Hill Police Site Design and Installation

AGENCY: U.S. Army
POINT OF CONTACT: Product Manager,
Physical Security Equipment
PHONE NUMBER: (703) 704-2416

PROJECTED ACCOMPLISHMENTS

FY98

- Completed installation at Fort Bliss (5/98)
- Completed Installation at Ft. Campbell (4/98)
- Completed Installation at Vicenza, Italy (3/98)
- Completed Final Design (4/98) and Commence Installation at Ft. Myer (6/98) and McNair (1 Jun 98)
- Issue ICIDS II Delivery Orders for Pine Bluff Arsenal and Pueblo Depot Activity
- Complete Installation of Capitol Hill Site - Phase I
- Issue new D.O. for Phase II of Capital Hill Site (6/98)

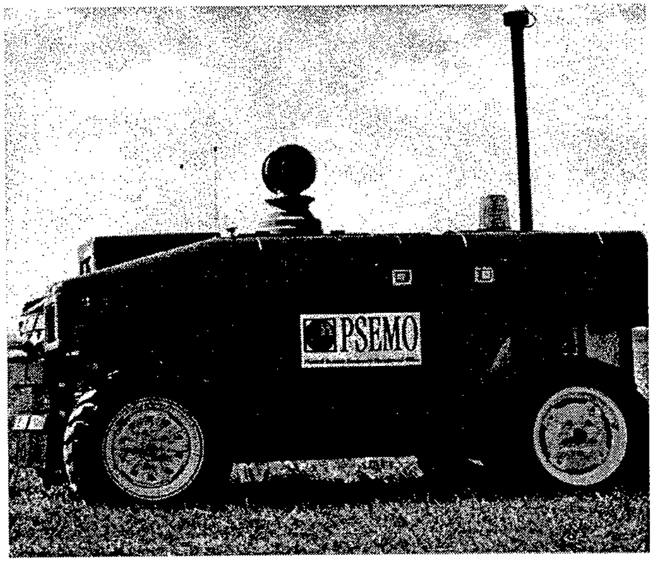
FY99

- Complete Final Design and Commence Installation at Fort Lewis, Pine Bluff Arsenal and Pueblo Depot Activity
- Issue ICIDS II Delivery Orders for Fort Lewis, WA and Blue Grass
- Complete Installation of Fort's Myer and McNair

5/19/98

MOBILE DETECTION ASSESSMENT RESPONSE SYSTEM - EXTERIOR (MDARS-E)

SUPPORTING MAJOR PROGRAM TITLE: MOBILE DETECTION ASSESSMENT RESPONSE SYSTEM



DESCRIPTION/OBJECTIVE

The MDARS-E is being designed to operate in general storage yards, arsenals, petroleum storage areas, airfields, rail yards and port facilities. MDARS-E will randomly navigate exterior perimeters and roadways, while performing intrusion detection, barrier assessment, visual assessment and audio response. Future Pre-Planned Product Improvements (P3I) will include employing delay devices and integrating all fixed exterior sensor and mobile platforms into a single system.

SIGNIFICANT ACCOMPLISHMENTS - FY97

- Successfully Completed Informal Vehicle Test at ATC Robotics Test Course
- Completed and Prototyped First Design Iteration of Internal Locking Device (ILD)
- Completed Initial Design and Integration of Vehicle Mission Payloads and Subsystems
- Conducted Design Review and Demonstration of Integrated Vehicle with Subsystems
- Integrated Sarnoff VFE-100 Collision Avoidance and IDS Subsystem into Vehicle

AGENCY: U.S. Army
POINT OF CONTACT: Product Manager,
Physical Security Equipment
PHONE NUMBER: (703) 704-2416

PROJECTED ACCOMPLISHMENTS

FY98

- Complete Initial Development of Command and Control Capabilities for MDARS-E Vehicle into the MDARS Console (MRHA)
- Complete Second Design Iteration and Prototype the ILD
- Install ILD at Initial Operational Evaluation Site

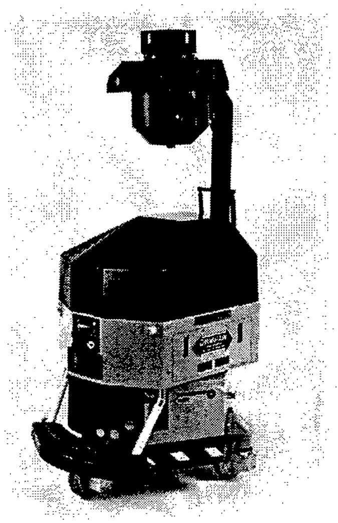
FY99

- Conduct Final Demonstration of 6.3 Prototype
- Conduct Development Testing
- Conduct MS I/II In Process Review
- Release Solicitation for 6.4 Prototype

5/19/98

MOBILE DETECTION ASSESSMENT RESPONSE SYSTEM - INTERIOR (MDARS-I)

SUPPORTING MAJOR PROGRAM TITLE: MOBILE DETECTION ASSESSMENT RESPONSE SYSTEM



DESCRIPTION/OBJECTIVE

The MDARS-I is being designed to operate in warehouses, office buildings, hospitals and other enclosed structures where personnel or property need protection. MDARS-I will randomly navigate building interiors while performing intrusion detection, inventory assessment, visual assessment and audio response. Future Pre-Planned Product Improvements (P3I) will include employing delay devices and integrating all fixed interior sensor and mobile platforms into a single system.

SIGNIFICANT ACCOMPLISHMENTS - FY97

- Developed Draft Specification and Draft RFP Components for EMD/Production Contract
- Anniston Army Depot Selected as EUA Site
- Successfully Completed Technical Feasibility Test-II
- Completed MDARS-I Platform Development and Prototyping
- Completed Installation Phases of MDARS-I EUA
- Developed EUA Evaluation Plan for the Product Assessment Subsystem
- Prepared IPR and RFP Packages

AGENCY: U.S. Army
POINT OF CONTACT: Product Manager,
Physical Security Equipment
PHONE NUMBER: (703) 704-2416

PROJECTED ACCOMPLISHMENTS

FY98

- Conduct System Functional Review (SFR)
- Complete Final Development of MDARS-I Command and Control Capabilities of the MDARS Console (MRHA)
- Conduct In-Process Review
- Conduct Early User Appraisal
- Release EMD RFP, Conduct EMD Source Selection

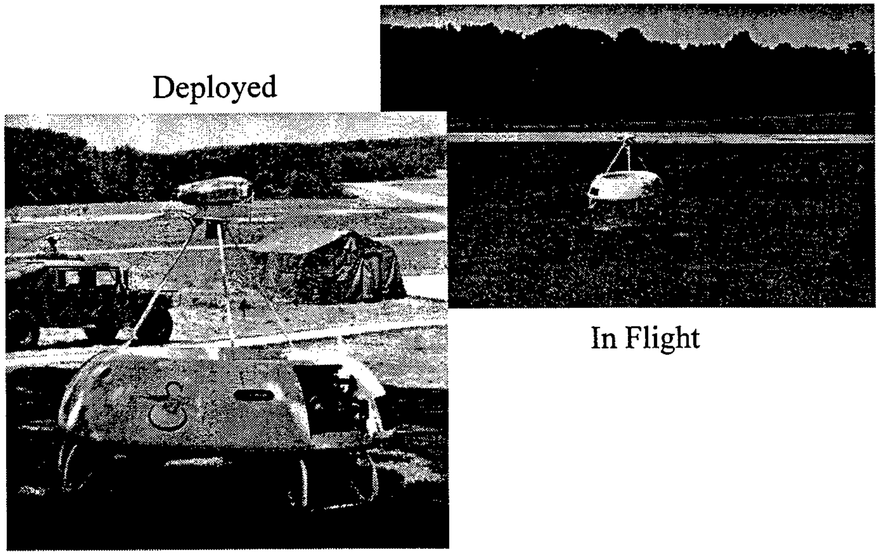
FY99

- Award EMD Contract (CPIF) with Production Options (FFP/FPI)
- Conduct TT/OT

5/19/98

MULTIPURPOSE SECURITY SURVEILLANCE MISSION PLATFORM (MSSMP)

SUPPORTING MAJOR PROGRAM TITLE: TACTICAL SECURITY EQUIPMENT



Deployed

In Flight

DESCRIPTION/OBJECTIVE

The MSSMP is designed to enhance Tactical Security and Force Protection through Extended Range Surveillance, Area (Sector) Intrusion Detection, Assessment and Identification. The major component of MSSMP is an air-mobile platform capable of vertical takeoffs and landings. As many as three MSSMP platforms will be controlled and monitored from a command control station mounted in the towing HMMWV. This station consists of a control and display subsystem as well as communications and navigation equipment. The air-mobile platforms must operate autonomously with minimum operator supervision.

SIGNIFICANT ACCOMPLISHMENTS - FY97

- Draft MSSMP MNS Developed by USAMPS and Submitted for Comment Worldwide
- MSSMP Submitted as Candidate for the MOUT ACTD: Nov 96
- Successfully Conducted MSSMP Experiments at MOUT Facility, Ft. Benning, GA
- Continued Integration of Platform and MPP C2 Consoles
- Incorporated Acoustic Sensor Capability into MPP

AGENCY: U.S. Army
POINT OF CONTACT: Product Manager,
Physical Security Equipment
PHONE NUMBER: (703) 704-2416

PROJECTED ACCOMPLISHMENTS

FY98

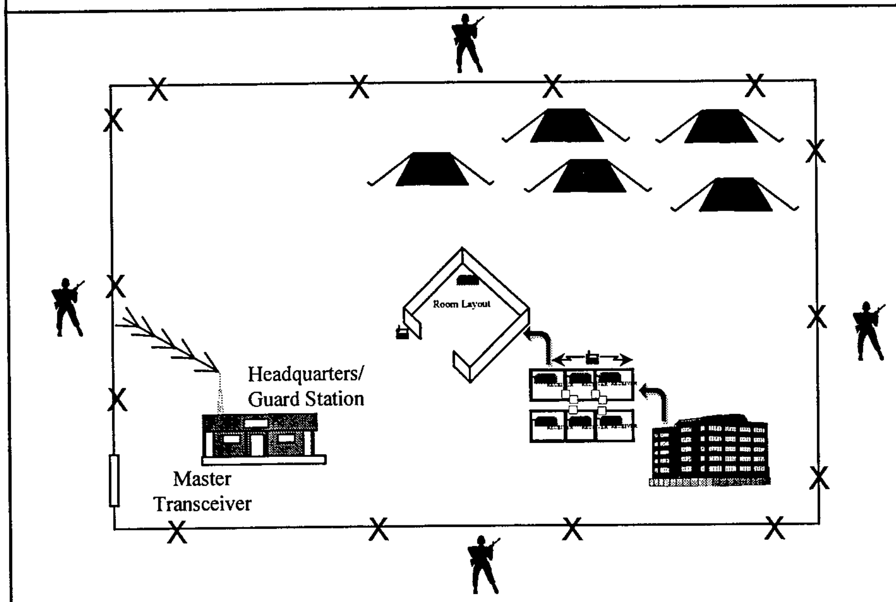
- Conduct Non-Lethal Technology Experiments with the MSSMP
- Incorporate Rotor Blade Design Changes for More Robust Platform Performance
- Participate in MOUT ACTD at Ft. Benning, GA.
- Support the Infantry Commander Conference 9-11 June 1998

FY99

- Continue participation in the MOUT ACTD

PERSONNEL ALERTING SYSTEM (PAS)

SUPPORTING MAJOR PROGRAM TITLE: TACTICAL SECURITY EQUIPMENT



DESCRIPTION/OBJECTIVE

PAS is being developed to provide a means to immediately alert personnel of specific danger (explosive, chemical, and biological agents) and provide intelligible communications on essential actions. Although centrally controlled, PAS will allow for remote activation by guard personnel. PAS will have worldwide applicability to include desert, tropical, and urban environments.

SIGNIFICANT ACCOMPLISHMENTS - FY97

- J-34 Releases Technology Request
- Commercial Off The Shelf Working Group Assigns Army As Lead Service
- Commerce Business Daily (CBD) Announcement Completed In September 1997

AGENCY: U.S. Army
POINT OF CONTACT: Product Manager,
Physical Security Equipment
PHONE NUMBER: (703) 704-2416

PROJECTED ACCOMPLISHMENTS

FY98

- 11 Firms Responded to CBD Announcement
- 3 Firms Selected For Final Evaluation
- Fort Belvoir Selected As Evaluation Site
- Operational and Laboratory Evaluation Initiated June 1998
- Completion Scheduled for July 1998

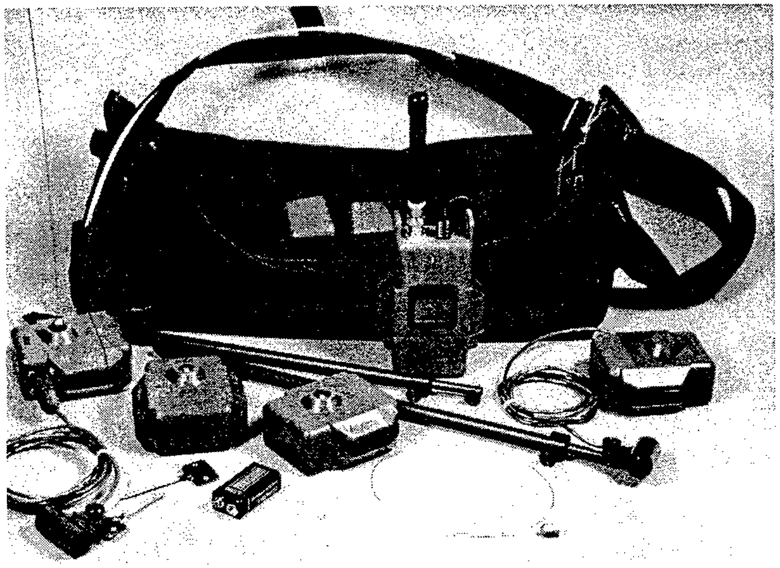
FY99

- Results will be added to the DoD Force Protection Physical Security Equipment Technology Guide

5/19/98

PLATOON EARLY WARNING DEVICE II (PEWD II)

SUPPORTING MAJOR PROGRAM TITLE: TACTICAL SECURITY EQUIPMENT



DESCRIPTION/OBJECTIVE

PEWD II will provide a replacement Tactical Sensor System for the Platoon Early Warning System (PEWS). The System requires the capability for early detection of vehicles and personnel to enhance soldier survivability during defensive and ambush type operations. By providing early detection of an enemy threat, this capability will enhance time available to determine the appropriate tactical response. The envisioned system would be organic to appropriate tactical units and available under Common Table and Allowances (CTA) to other forces to meet contingency missions. Emphasis should be placed on ease of deployment, operation, and recovery.

SIGNIFICANT ACCOMPLISHMENTS - FY97

- USAIC Designated the Combat Developer
- ORD Approved by TRADOC/PM-PSE assigned as Material Developer
- Initiated Market Investigation to Identify NDI/COTS Systems Candidates
- Conducted Initial Technical Testing on 4 Potential Candidate NDI/COTS Systems
- Developed draft Acquisition Strategy and Plan

AGENCY: U.S. Army
POINT OF CONTACT: Product Manager,
Physical Security Equipment
PHONE NUMBER: (703) 704-2416

PROJECTED ACCOMPLISHMENTS

FY98

- Develop Program Management Plan
- Evaluate Candidate NDI/COTS Systems Including Air Force TASS to Determine Requirement Shortfalls
- Initiate Market Investigation

FY99

- Conduct Trade-off Analysis and Trade-off Determination
- Develop Logistics Concept

5/19/98

FORCE PROTECTION
COMMON OPERATIONAL PICTURE / COMMON TACTICAL PICTURE

14TH ANNUAL SECURITY TECHNOLOGY SYMPOSIUM AND EXHIBITION

COLONEL RUSSELL N. PETER, ESC/FD
5 EGLIN STREET
BUILDING 1624
HANSCOM AFB, MA 01731-2308
PHONE: (781) 377-6002
FAX: (781) 377-8832
E-MAIL: peterr@hanscom.af.mil

Force Protection Common Operational Picture/Common Tactical Picture

25 June 1996: The Wake Up Call

At 2153 hours local, a truck bomb exploded at the Khobar Towers compound near Dhahran and killed 19 service members. Khobar Towers was the residential quarters of almost 3,000 US military personnel of the 440th Air Wing (Provisional).

William J. Perry, Secretary of Defense, in his Report to the President and Congress on the Protection of U. S. Forces Deployed Abroad on 15 September 1996 said: "...the Khobar Towers attack should be seen as a watershed event pointing the way to a radically new mindset and dramatic changes in the way we protect our forces deployed overseas from this growing threat."

In response to this attack and the growing potential for more attacks by terrorists, irregular forces, and disenchanted employees against its bases and facilities and personnel, the Air Force has taken an integrated approach to Force Protection. There is a recognition that Force Protection is not a Security Police operation; but is a Security Force operation. This exemplifies a mindset change and a movement away from pure law enforcement and stovepipe operations to an integrated Security Force for Force Protection. This is evidenced by the formation last year of the 820th Security Forces Group (SFG) with its mix of security force, office of special investigations (OSI), intelligence, medical, communications, civil engineering, and logistics and supply personnel and the Force Protection Battlelab with a similar mix of personnel. The Air Staff now has a Security Force directorate (SAF/SF) and the Security Forces Center has been established at Lackland AFB, TX.

The threat to our bases and facilities is multi-dimensional. It could manifest itself as a medical attack; an information warfare attack; a chemical, biological, or nuclear weapon attack; a military operation (ground, air, and/or sea attack); a sapper attack; or any combination thereof. In the past, these incidents or attacks would have been reported within stovepipe channels; but, as highlighted by the Downing Report on Khobar Towers which stated there was a requirement for the infusion of intelligence support for Force Protection operations, the Force Protection mission area must have an integrated approach for providing situation awareness to our Security Force elements. These elements must have an understanding of the theater/regional Force Protection (FP) environment for uncommitted forces, as well as a local situation awareness picture, much as is done for the engaged forces within the Global Command and Control System (GCCS) Common Operational Picture. To address this need, the Force Protection C2 Systems program office at Hanscom AFB, MA (ESC/FD) has initiated a proof-of-concept testbed effort modeled after the Common Operational Picture concept - the Force Protection Common Operational Picture/Common Tactical Picture (COP/CTP). (The definitions for the GCCS COP and CTP are attached.)

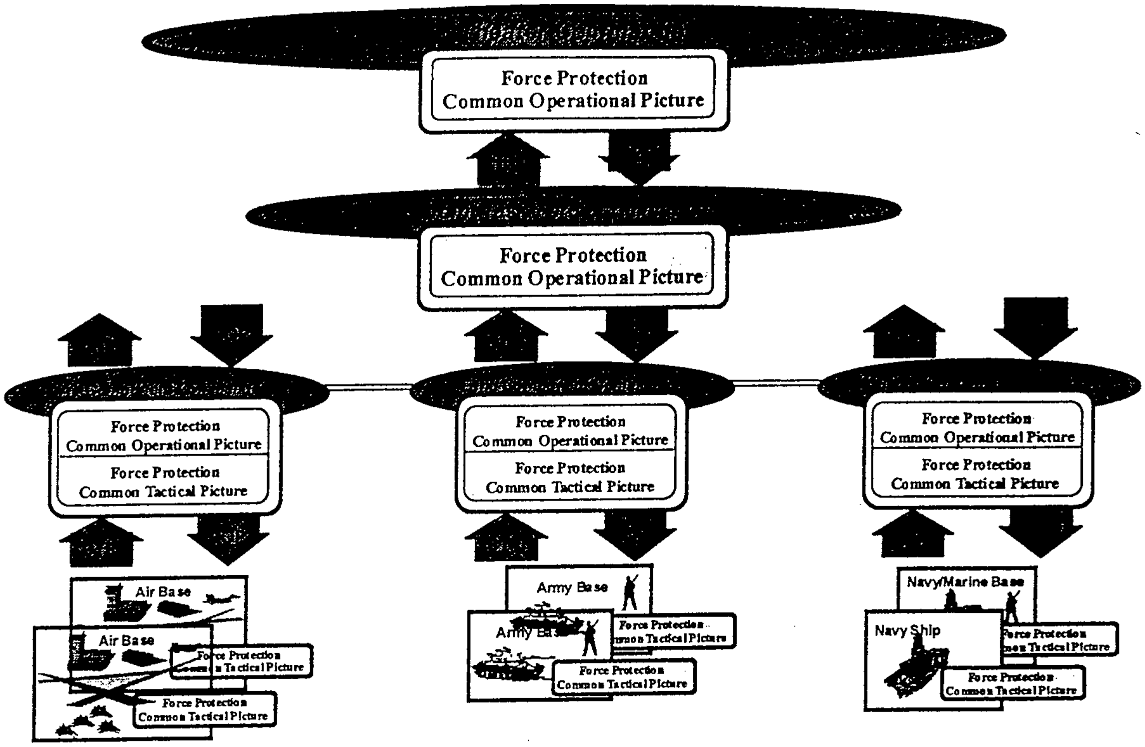

Force Protection Common Operational Picture
Force Protection Common Operational Picture
Force Protection Common Operational Picture
Force Protection Common Tactical Picture
Force Protection Common Operational Picture
Force Protection Common Tactical Picture
Force Protection Common Operational Picture
Force Protection Common Tactical Picture
Air Base
Air Base
Force Protection Common Tactical Picture
Force Protection Common Tactical Picture
Army Base
Army Base
Force Protection Common Tactical Picture
Force Protection Common Tactical Picture
Navy/Marine Base
Navy Ship
Force Protection Common Tactical Picture
Force Protection Common Tactical Picture

Figure 1: Joint Force Protection Tailored Awareness

Description:

The Air Force Security Forces have established five integrated protection zones around their facilities and personnel in order to characterize protection needs, information flows, and areas of responsibility: airman, perimeter, tactical, detection, and intelligence.

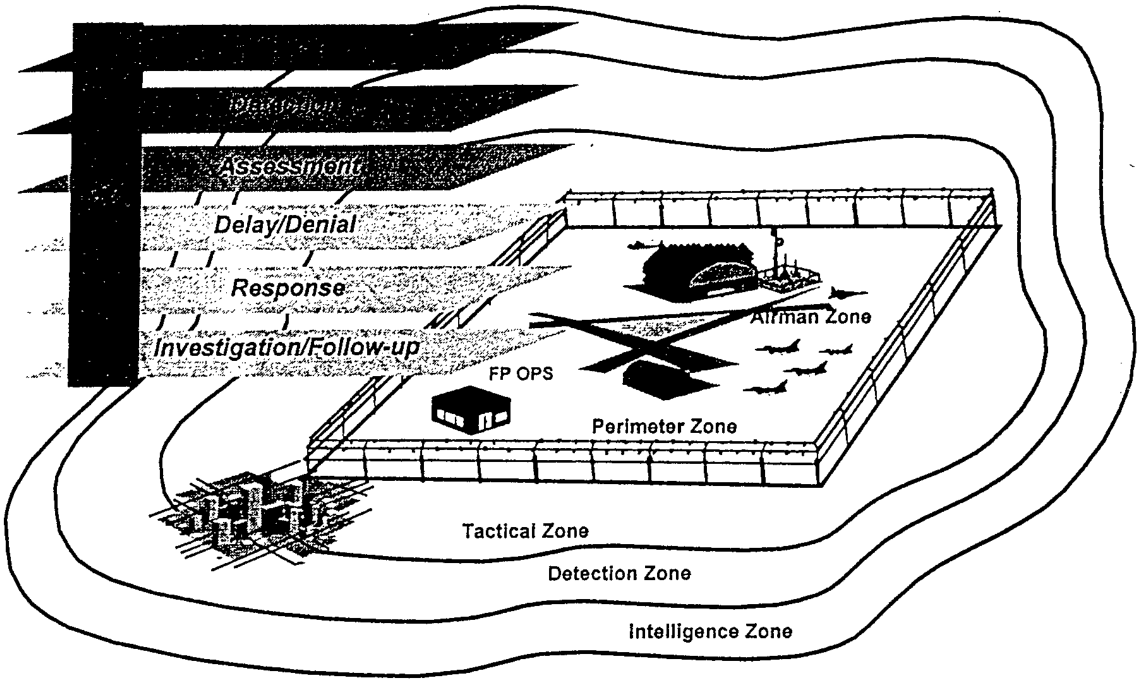
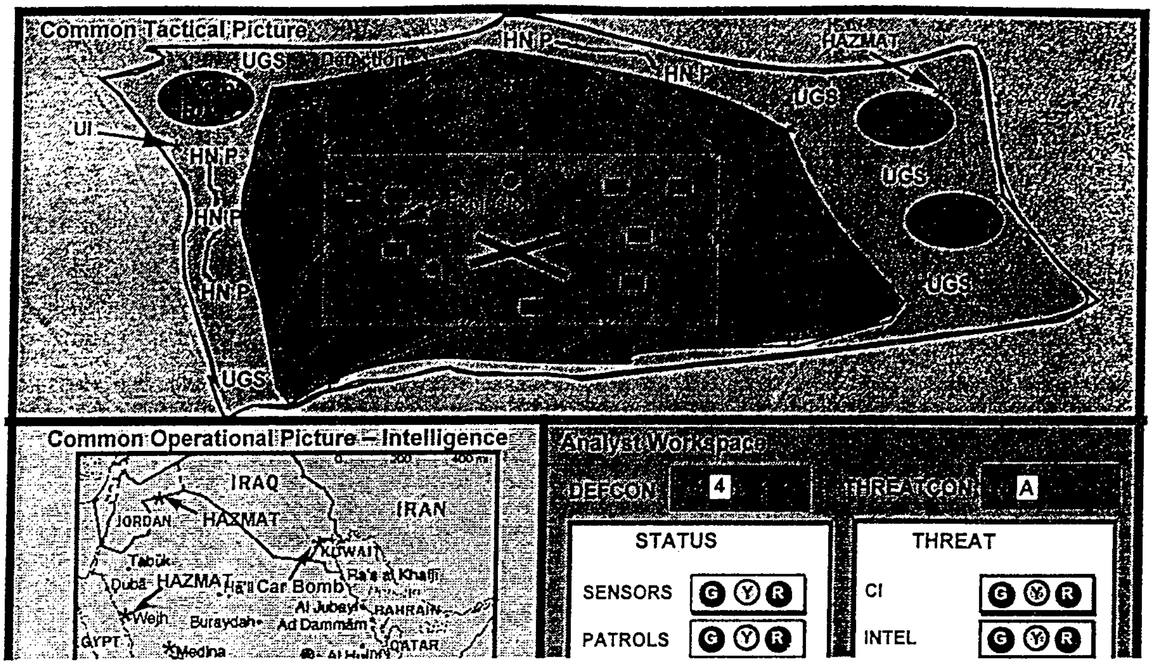


Figure 2: The Force Protection World Tactical View

The FP COP provides a view of the FP intelligence zone. Portrayed are incidents, such as fires, hazardous material detections, kidnappings, intrusions or events at other installations, as well as global trends of activities of terrorist, irregular force, or disenchanted elements. Global weather and global news, as provided by CNN-type organizations and news services, related to the Force Protection mission area are also presented as part of this COP. Additionally, it is envisioned that General Military Intelligence topics of interest, such as new weapons and their functionality and regional terrorist organizational structures, capabilities, and personalities would also be covered as part of the COP. The FP COP would be a joint force product created at the Joint Task Force (JTF)/Theater Commander in Chief (CINC) level and disseminated to the service component security forces throughout the area of responsibility.



DEFCON 4

THREATCON A

SENSORS G Y R

PATROLS G Y R

CI G Y R

INTEL G Y R

Figure 3: Force Protection Common Operational Picture/Common Tactical Picture

Also contributing to the COP, would be the local installation's Common Tactical Picture (CTP). This is the coverage of the airman, perimeter, tactical, and detection zones around the base. It is envisioned that changes in the status of the base infrastructure (utilities) would be integrated with inputs from surveillance systems (such as the Tactical Automated Security System (TASS) and Unattended Ground Sensors (UGSs), Unpiloted Aerial Vehicles (UAVs), and patrols); intelligence and OSI reports; reports of local incidents and events (fires, explosions, subversion, medical alerts, etc.); information attacks; and host/local nation information to provide this CTP. The CTP from multiple installations throughout the region/theater would be a contributor to the COP. Additionally, the CTP would include local weather and base operational status, such as planned operations and runway usage.

Associated with maintenance of the Force Protection COP/CTP at the unit level is the analyst area of the COP/CTP display. This area provides support to the COP/CTP operator. It provides checklists, Standing Operating Procedures, position logs, and other support capabilities. Additionally, it eventually will provide rule or knowledge-based support for combining seemingly unrelated incidents/events into a meaningful entry for the CTP. It could also offer the opportunity to perform vulnerability and "what if" analyses.

It is envisioned that there would be possibly four components/anchor desks that would contribute to the CTP and benefit from its presentation of integrated information: Sensor Integration Cell, Intelligence/Counter Intelligence (Intel/CI) Cell, Base Status/Vulnerability Assessment Cell, Civil Military/External Cell. The Security Force (SF) battle manager would be located in the Base Defense Operations Center (BDOC) and would coordinate both the detection, identification, location, and characterization of the threat , as well as the response to a potential or actual action against the base.

It is envisioned that there would be possibly four components/anchor desks that would contribute to the CTP and benefit from its presentation of integrated information: Sensor Integration Cell, Intelligence/Counter Intelligence (Intel/CI) Cell, Base Status/Vulnerability Assessment Cell, Civil Military/External Cell. The Security Force (SF) battle manager would be located in the Base Defense Operations Center (BDOC) and would coordinate both the detection, identification, location, and characterization of the threat, as well as the response to a potential or actual action against the base.

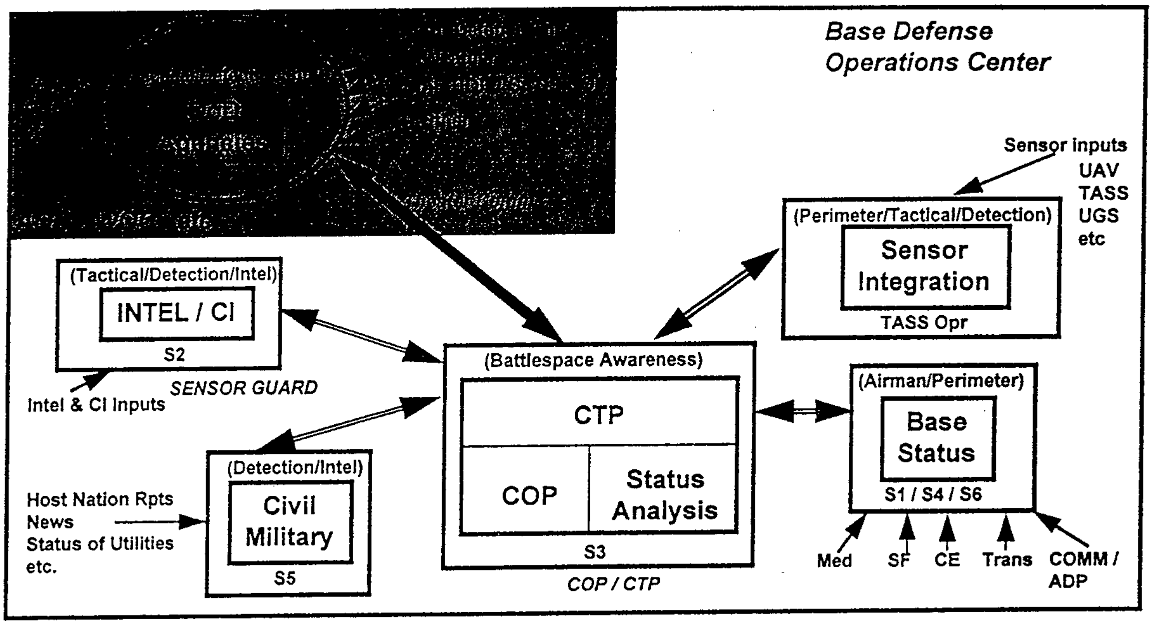


Figure 4: FP Battle Management C2: Unit Level

The Sensor Integration Cell (a permanent cell) would provide the situation awareness picture by the integration of the inputs from the supporting sensors systems, e. g., chem/bio detectors, TASS, UGS. This cell could task sensors to change coverage or add additional sensors. By controlling the sensors, it will be able to optimize coverage against potential types and locations of threats. Its contribution to the CTP would be the integrated Sensor Picture (Situation Awareness picture). The Intel/CI Cell (a permanent cell) would correlate the HUMINT and national sensor inputs, as well as facilitating the submission of Requests For Information (RFI) in support of the Collection Management process. It would be this cell's responsibility to task collection assets for additional information, query INTELINK/INTELINK-S for information, and query the various CI systems for additional information on terrorist and other groups/individuals. Its part of the CTP would be an adjunct to the Sensor Integration Cell input in order to clarify threat potential capabilities or threats in the area. The Base Status/Vulnerability Assessment Cell (possibly an "on call" cell) would be responsible for identifying and characterizing the critical infrastructures on the base that support base operations and the critical aspects of the base's mission. They would contribute information as to what areas need protection and how they should be protected. This would affect the sensor coverage program managed by the Sensor Integration Cell. Additionally, once the Sensor Integration Cell and/or Intel/CI cell have characterized a threat, the Base Status Cell will be able to forecast intentions and areas of the infrastructure that are directly under attack or threat of attack and the impact of that attack. This cell would contribute annotated base diagrams/drawings and/or alerts (e. g., medical) to indicate infrastructure areas under actual or potential threat attack. The Civil Military/External Cell (possibly an "on call" cell) would provide information from the local police, other services, other bases, etc. that are external to the base which also may have a significant impact on the base's force protection. Its input to the CTP may be on the order of refugee movements, locations of disturbances or dissidents, other bases having attacks as a graphical overlay, status of host nation response assets (police, fire, disaster relief, etc.) and status of host nation utilities supporting the base or facility.

Development and Schedule:

Our basic approach for the development of this testbed capability is to use, as much as possible, COTS/GOTS products that are compatible with the Windows NT operating environment, per the request of our immediate user - the 820th Security Forces Group. Currently, our effort is divided into three phases so that we can continuously involve our user in our spiral development process and help the user to better define their requirements for this capability. The end goal is to use our collective experience from this testbed effort to publish a Request For Proposal for the productization of the Force Protection COP/CTP that will meet the needs of Security Force elements in any MAJCOM and, possibly the Joint arena. The following describes the phased development of this activity and anticipated completion dates. Phase I activity will be driven by the input of simulated data. The dates for phases II and II may change based on the immediate needs of the user and user operational requirements, as well as operator feedback on the previous phase's capabilities.

- Phase I: Initial Integration and CTP Development
SEP 98

- - Investigate the utility of advanced Mapping, Cartographic, and Geodesy (MC&G) capabilities and other display tools

- - Integration of the output of the TASS and tactical alerting and reporting system to provide the local situation awareness picture to create the Sensor Integration Cell

-- Start integration of Joint Warning and Reporting Network (JWARN) capability

- Phase II: COP Integration and Enhanced CTP Capability
SEP 99

-- Incorporate user feedback from Phase I to enhance the CTP

-- Investigate applicability and incorporation of multi-level security capabilities

-- Continue JWARN implementation, as it matures

-- Investigate integration with the Wing Command and Control System (WCCS)

-- Investigate incorporation of the Counter Intelligence Deployable System (CIDS) or other Counter Intelligence capabilities

-- Integrate SENSOR GUARD (a FP deployable intel capability) into the COP/CTP construct as the Intel/CI Cell

- Phase III: COP and CTP Enhancement SEP 00

-- Develop analyst support tools using rule-based or knowledge-based capabilities, timeline analysis capability, etc. for development of Analyst Area

-- Integrate JWARN control of CBR detectors into Sensor integration Cell

-- Integrate vulnerability assessment tools, medical reporting, SF reporting into Base Status Cell

-- Develop Civil Military/External Cell capability

Issues/Challenges:

- FP COP: As the Force Protection mission area matures, there will be a need for the FP COP to be defined and disseminated to the Security Forces within Theater in the same manner as the GCCS COP

- The FP COP/CTP must be brought under the umbrella of the GCCS as a Joint application. It should be a layer on the GCCS COP.

- Within the Air Force, the FP COP/CTP should be an application within Theater Battle Management Core System (TBMCS)

Future:

- The FP COP/CTP has applicability across all the services and should be made a Joint capability

- FP COP/CTP will be an experiment within the Expeditionary Forces Experiment - 99 in July 1999

Attachment: Definitions

Reference: CJCSI 3151.01, 10 June 1997, "Global Command and Control System Common Operational Picture Reporting Requirements"

Common Operational Picture. The COP is the integrated capability to receive, correlate, and display a Common Tactical Picture (CTP), including planning applications and theater-generated overlays/projections (i.e., Meteorological and Oceanographic (METOC), battleplans, force position projections). Overlays and projections may include location of friendly, hostile, and neutral units, assets, and reference points. The COP may include information relevant to the tactical and strategic level of command. This includes, but is not limited to, any geographically oriented data, planning data from JOPES, readiness data from SORTS, intelligence (including imagery overlays), reconnaissance data from the Global Reconnaissance Information System (GRIS), weather from METOC, predictions of nuclear, biological, and chemical (NBC) fallout, and Air Tasking Order (ATO) data.

Common Tactical Dataset. The CTD is a repository of data that contains all the information available to the JTF that will be used to build the COP and CTP. The CTD is not fused, correlated, or processed data in the sense that the information has not been scrutinized by the CCM [CINC COP Manager] or track managers for time value, redundancy, or conflicts. However, the CTD may contain processed intelligence data. The CTD is a major sub-component of the COP and refers to: the CINC designated repository for current battlespace information including disposition of hostile, neutral, and friendly forces as they pertain to US and multinational operations ranging from peacetime through crisis and war for the entire area of responsibility (AOR). Upon discretion of the CINC, the CTD may be a logical database vice physical if there are several JTFs or activities that will necessitate COP reporting. In these cases there may be more than one location of database storage.

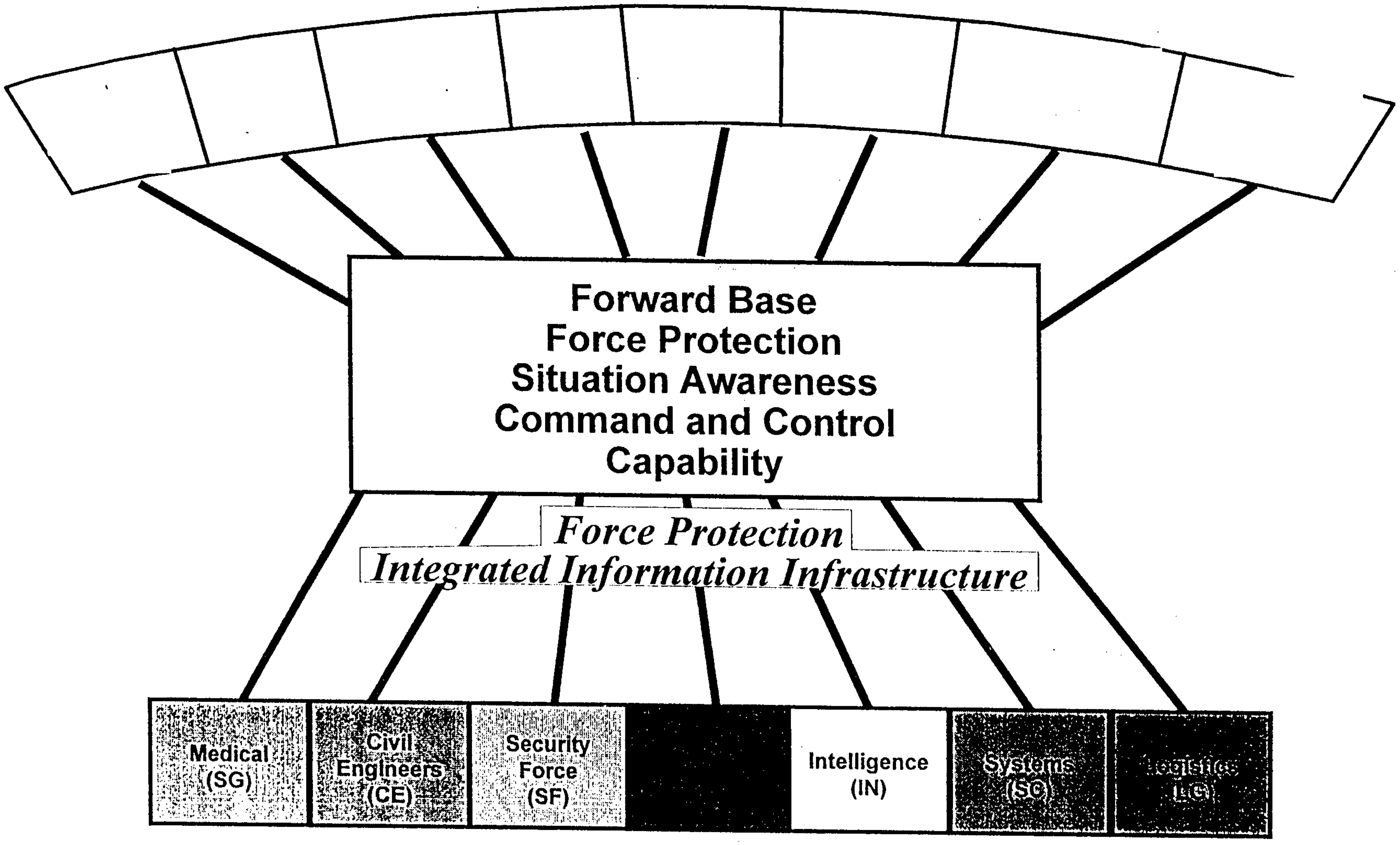
Common Tactical Picture. The CTP is derived from the CTD and other sources and refers to the current depiction of the battlespace for a single operation within a CINCis AOR including current, anticipated or projected, and planned disposition of hostile, neutral, and friendly forces as they pertain to US and multinational operations ranging from peacetime through crisis and war. The CTP includes force location, real time and non-real-time sensor information, and amplifying information such as METOC, SORTS [Status of Resources and Training System], and JOPES [Joint Operation Planning and Execution System].

Force Protection
Common Operational Picture/ Common Tactical Picture

Col Russell N. Peter
Program Director
ESC/FD
(781) 377-6002
peterr@hanscom.af.mil

Force Protection Goal

The Integrated Goal Capability

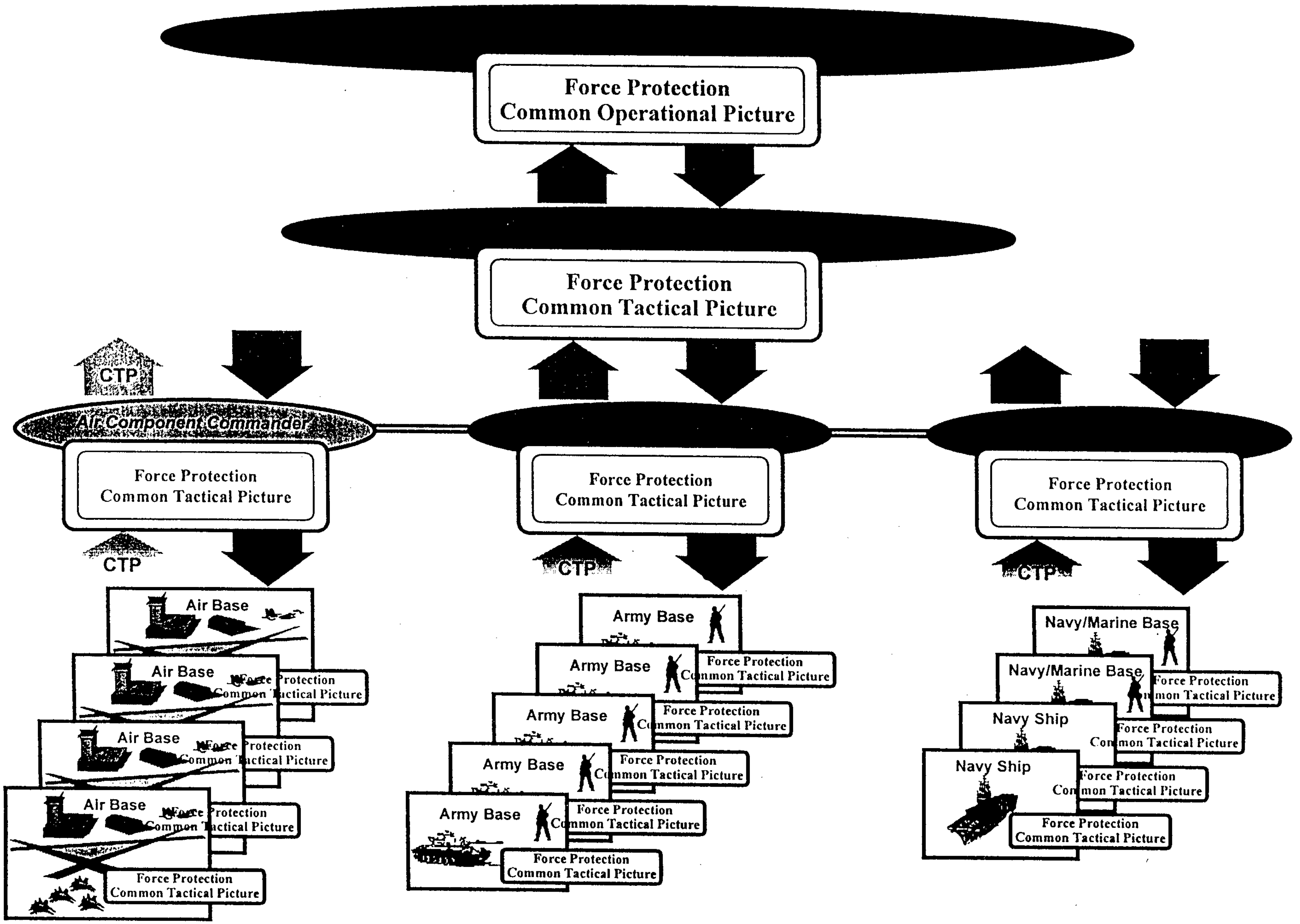


Forward Base
Force Protection
Situation Awareness
Command and Control
Capability

Force Protection
Integrated Information Infrastructure

PP-798
Draft

Joint Force Protection Tailored Awareness



Force Protection
Common Operational Picture

Force Protection
Common Tactical Picture

CTP

Air Component Commander

Force Protection
Common Tactical Picture

CTP

Air Base

Air Base

Air Base

Air Base

Force Protection
Common Tactical Picture

Force Protection
Common Tactical Picture

CTP

Army Base

Army Base

Army Base

Army Base

Army Base

Force Protection
Common Tactical Picture

Force Protection
Common Tactical Picture

CTP

Navy/Marine Base

Navy/Marine Base

Navy Ship

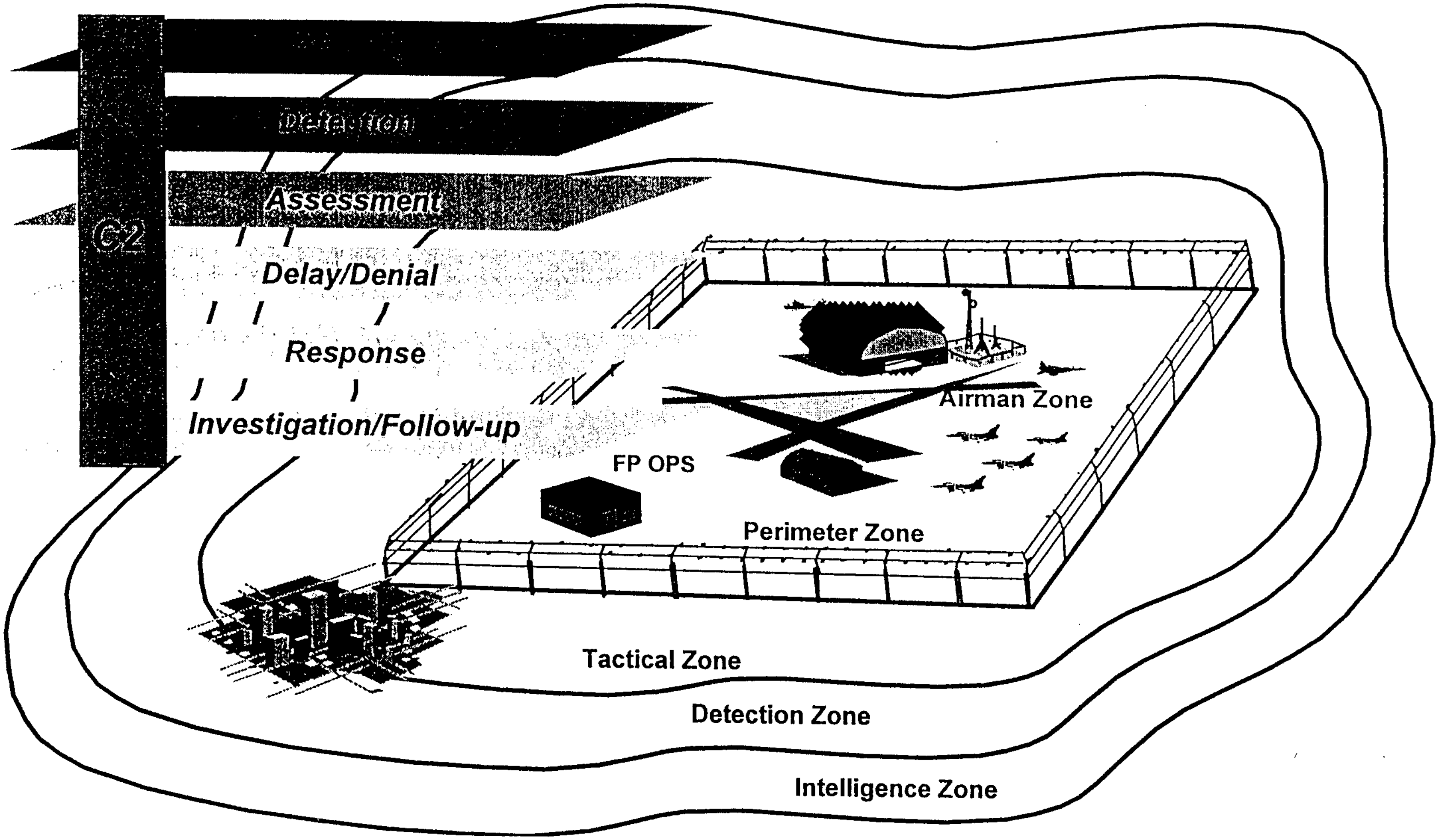
Navy Ship

Force Protection
Common Tactical Picture

The Force Protection World Tactical View

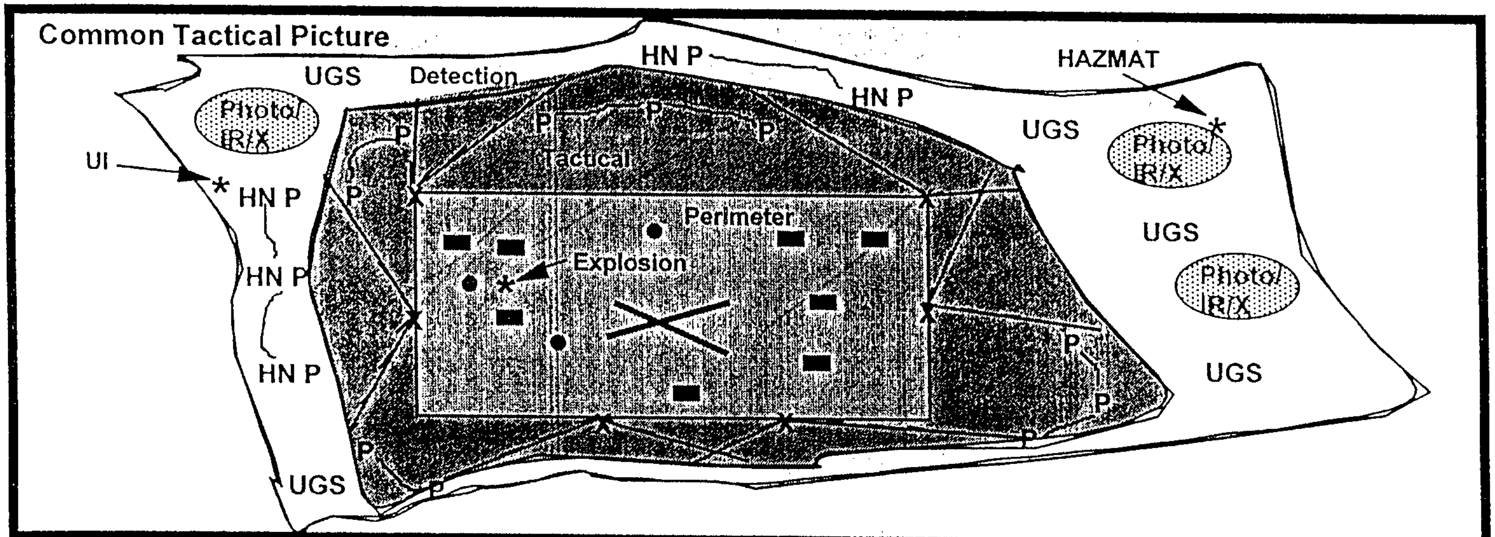
MISSION
Acquire, Deliver and *Sustain* Quality Integrated Command and Control *Systems* to Provide Force Protection to Warfighting Resources and to Government Agencies During Emergencies and Natural Disasters.

VISION
World Class Leader in Applying Technology to Force Protection C^2 Systems for the *Safety, Security* and *Survivability* of US Warfighting Assets, US *Warfighters* and Dependents Worldwide.

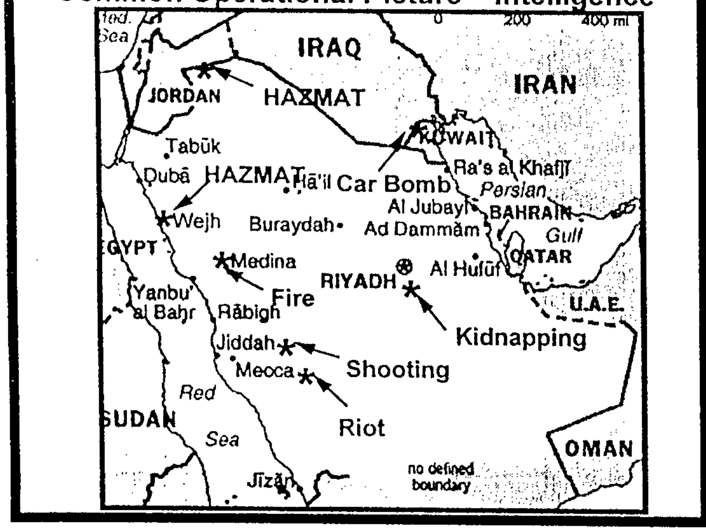


Force Protection
Common Operational Picture/Common Tactical Picture (COP/CTP)

Common Tactical Picture



Common Operational Picture – Intelligence



Analyst Workspace

DEFCON 5 4 3 2 1

THREATCON N A B C D

STATUS	
SENSORS	● Ⓨ ●
PATROLS	● Ⓨ ●
COMMS	● Ⓨ ●
UTILITIES	● Ⓨ ●
HOST N	● Ⓨ ●

THREAT	
CI	● Ⓨ ●
INTEL	● Ⓨ ●
HAZMAT	● Ⓨ ●
INFO WAR	● Ⓨ ●
INCIDENTS	● Ⓨ ●

Common Tactical Picture

- Overlay

Critical Nodes
Patrol (P) or HN P) Locations
Sensors & FOV (X)
Incidents
Key Utilities

- Imagery with Anotation
- Zoom
- Maps with Overlay
- Virtual Reality Picture

Common Operational Picture

- Wx
- Natural Disaster
- Tech Threats
- Incidents
- Imagery with Anotation
- Maps
- HyperLink to imagery/maps/etc
- CI Products
- GMI Products

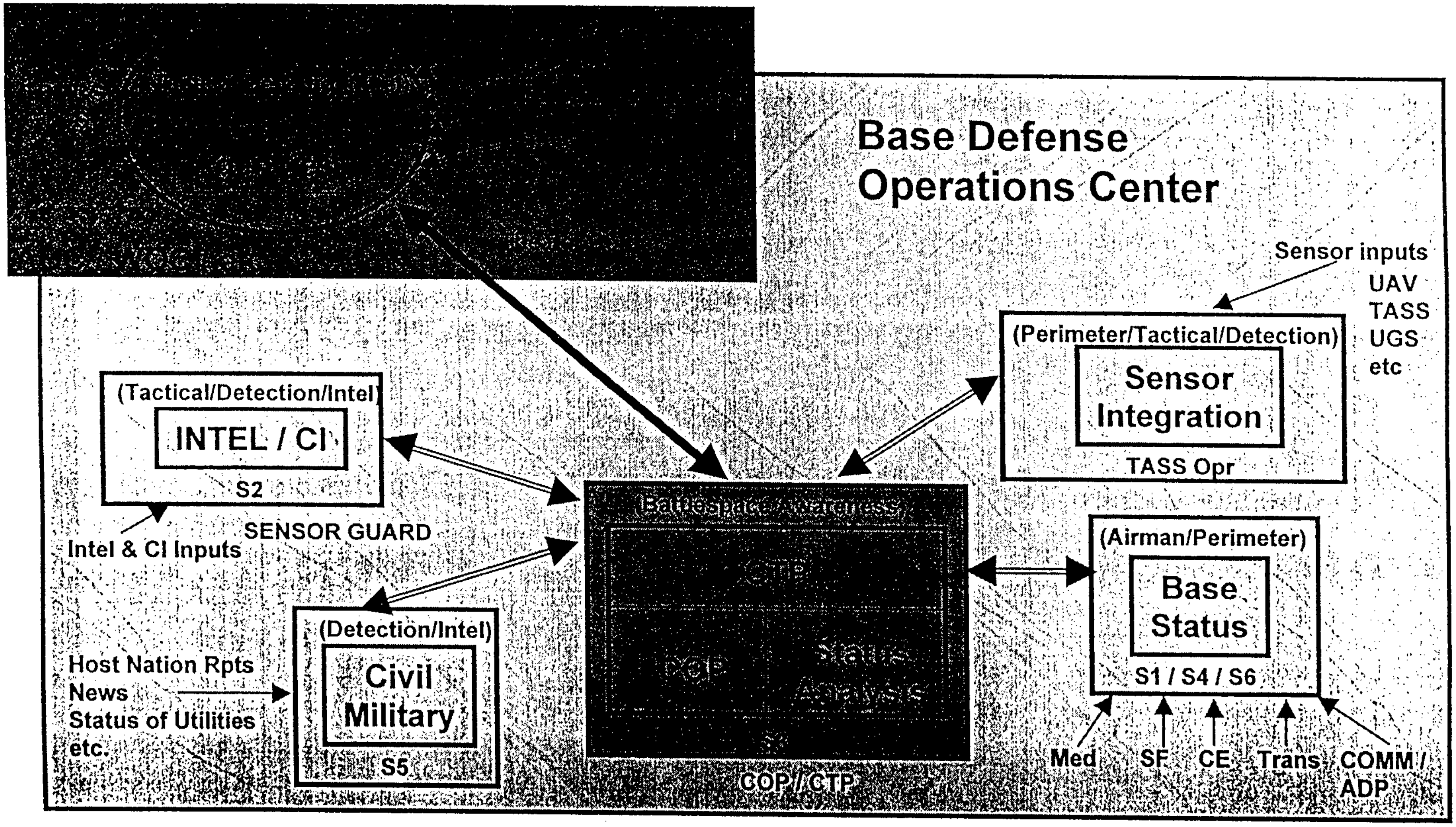
Analyst Work Area

- Buttons bring up text
- Menu

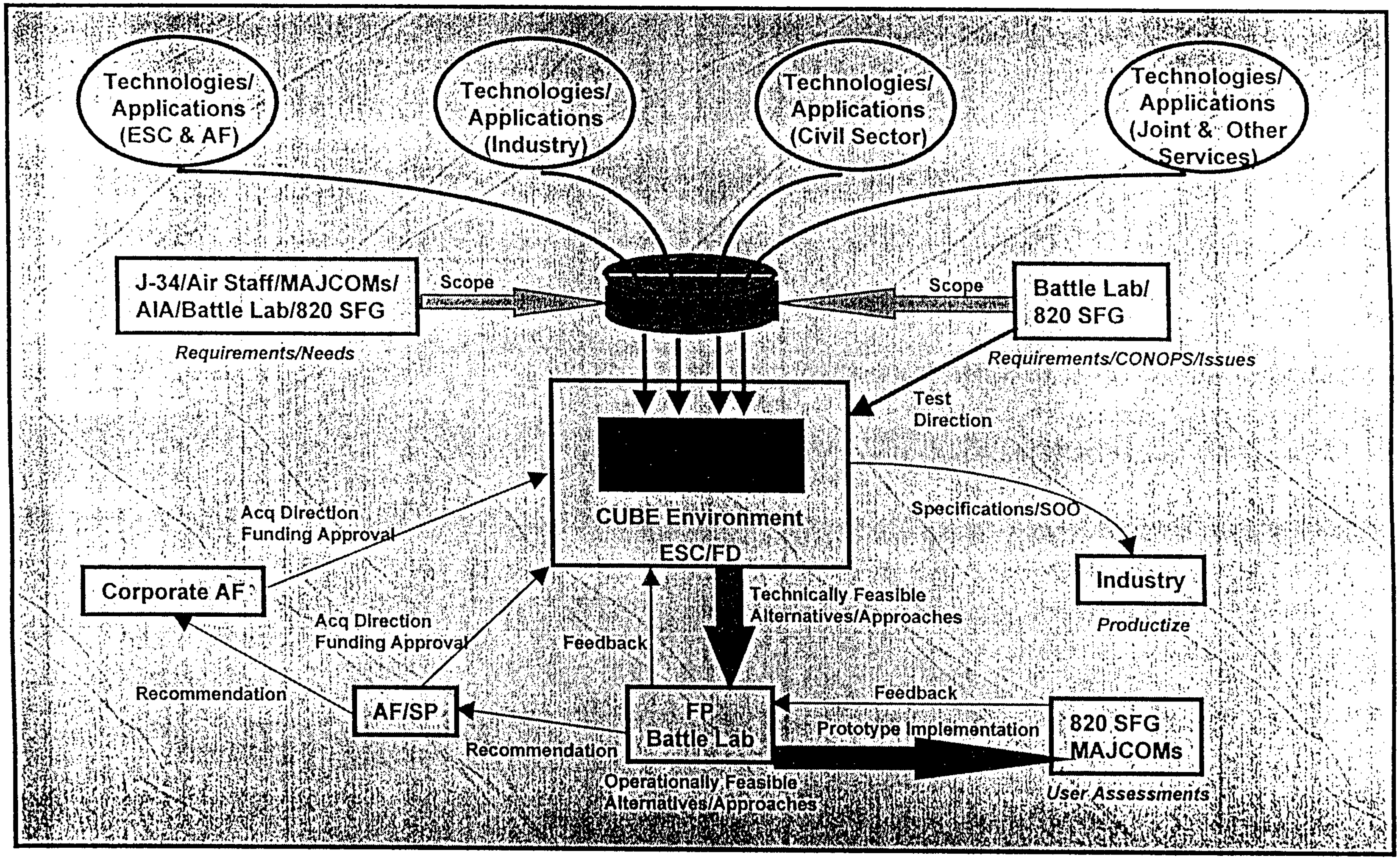
Checklist
Continuity Book
SOP
Auto Log
Assessments
USMTF Msgs

- Collaborative Capability

FP Battle Management C2: Unit Level



FP Testbed Process


Technologies/ Applications (ESC & AF)
Technologies/ Applications (Industry)
Technologies/ Applications (Civil Sector)
Technologies/ Applications (Joint & Other Services)
J-34/Air Staff/MAJCOMs/ AIA/Battle Lab/820 SFG
Scope
Requirements/Needs
Scope
Battle Lab/ 820 SFG
Requirements/CONOPS/Issues
Test Direction
CUBE Environment ESC/FD
Specifications/SOO
Industry
Productize
Acq Direction Funding Approval
Corporate AF
Acq Direction Funding Approval
Feedback
Technically Feasible Alternatives/Approaches
Recommendation
AF/SP
Recommendation
FP Battle Lab
Feedback
Prototype Implementation
820 SFG MAJCOMs
Operationally Feasible Alternatives/Approaches
User Assessments

COP/CTP

- Phase I: Initial Integration and CTP Development
  - MC&G capabilities and display tools
  - TASS input
  - Initial development of Sensor Integration Cell
- Phase II: COP Integration and Enhanced CTP
  - Use feedback
  - Multi-Level Security investigation
  - JWARN integration?
  - Investigate CI interfaces/integration
  - Implement SENSOR GUARD as Intel/CI Cell
- Phase III: COP and CTP Enhancement
  - Incorporate analyst support tools
  - Integrate JWARN control of detectors
  - Integrate Vulnerability Assessment tools
  - Develop Base Status Cell capability
  - Develop Civil Military / External Cell

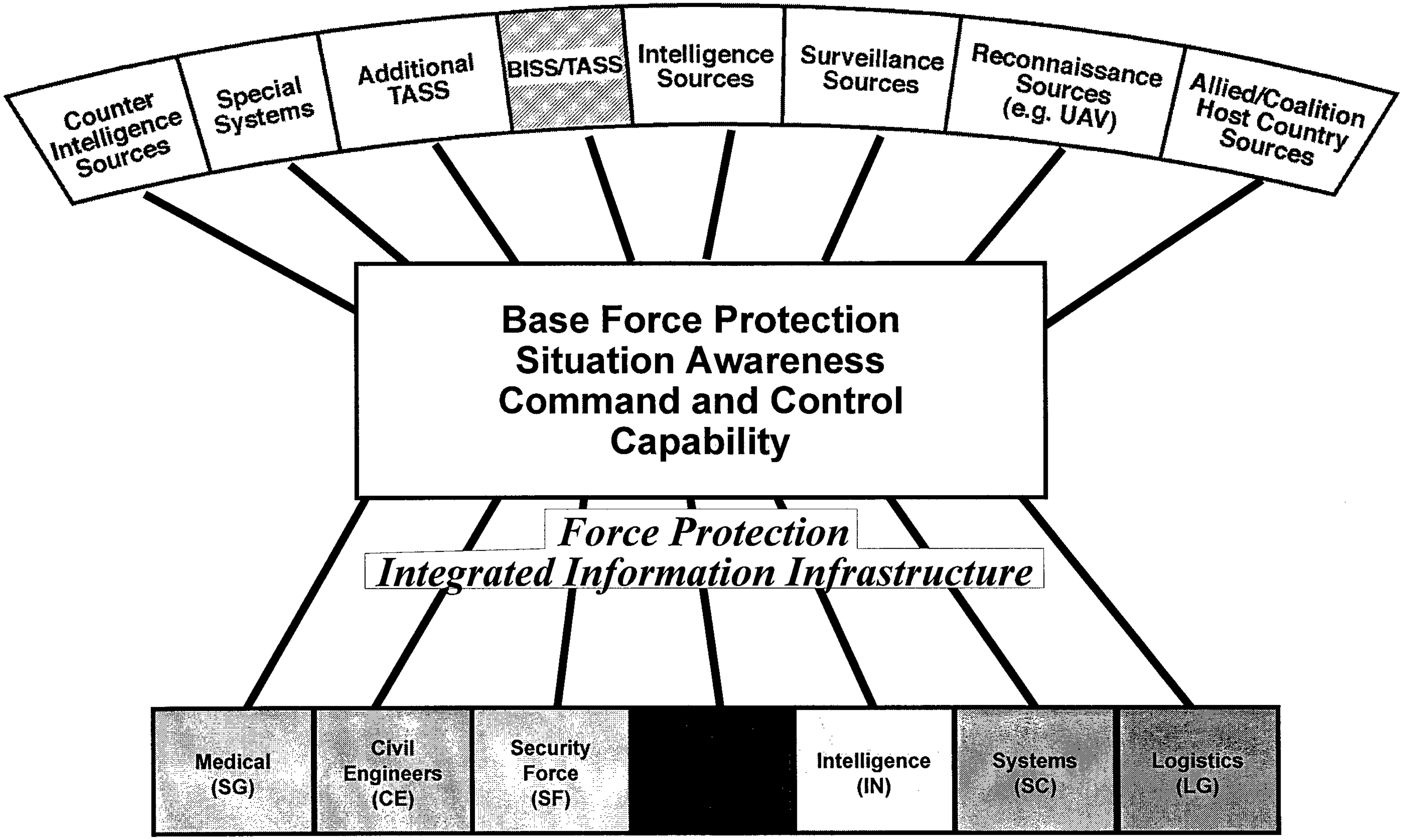
7/6/98

Force Protection
Common Operational Picture/ Common Tactical Picture

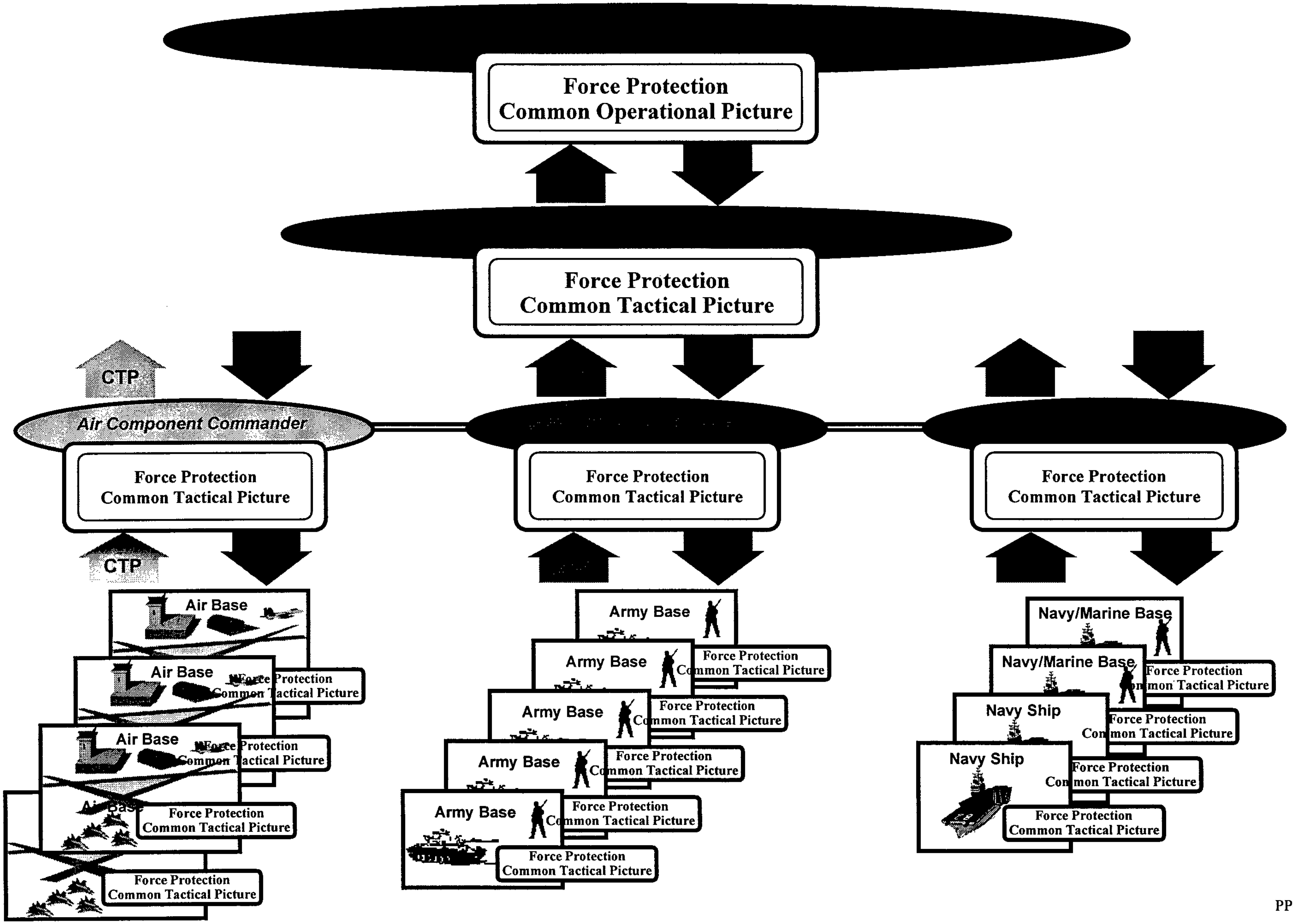
Col Russell N. Peter
Program Director
ESC/FD
(781) 377-6002
peterr@hanscom.af.mil

7/6/98

Force Protection
The Integrated Goal Capability


Counter Intelligence Sources
Special Systems
Additional TASS
BISS/TASS
Intelligence Sources
Surveillance Sources
Reconnaissance Sources (e.g. UAV)
Allied/Coalition Host Country Sources
Base Force Protection Situation Awareness Command and Control Capability
Force Protection Integrated Information Infrastructure
Medical (SG)
Civil Engineers (CE)
Security Force (SF)
[redacted]
Intelligence (IN)
Systems (SC)
Logistics (LG)

Joint Force Protection Tailored Awareness



Force Protection Common Operational Picture

Force Protection Common Tactical Picture

CTP

Air Component Commander

Force Protection Common Tactical Picture

CTP

Force Protection Common Tactical Picture

Force Protection Common Tactical Picture

Air Base

Air Base

Air Base

Air Base

Force Protection Common Tactical Picture

Force Protection Common Tactical Picture

Force Protection Common Tactical Picture

Force Protection Common Tactical Picture

Army Base

Army Base

Army Base

Army Base

Army Base

Force Protection Common Tactical Picture

Force Protection Common Tactical Picture

Force Protection Common Tactical Picture

Force Protection Common Tactical Picture

Force Protection Common Tactical Picture

Navy/Marine Base

Navy/Marine Base

Navy Ship

Navy Ship

Force Protection Common Tactical Picture

Force Protection Common Tactical Picture

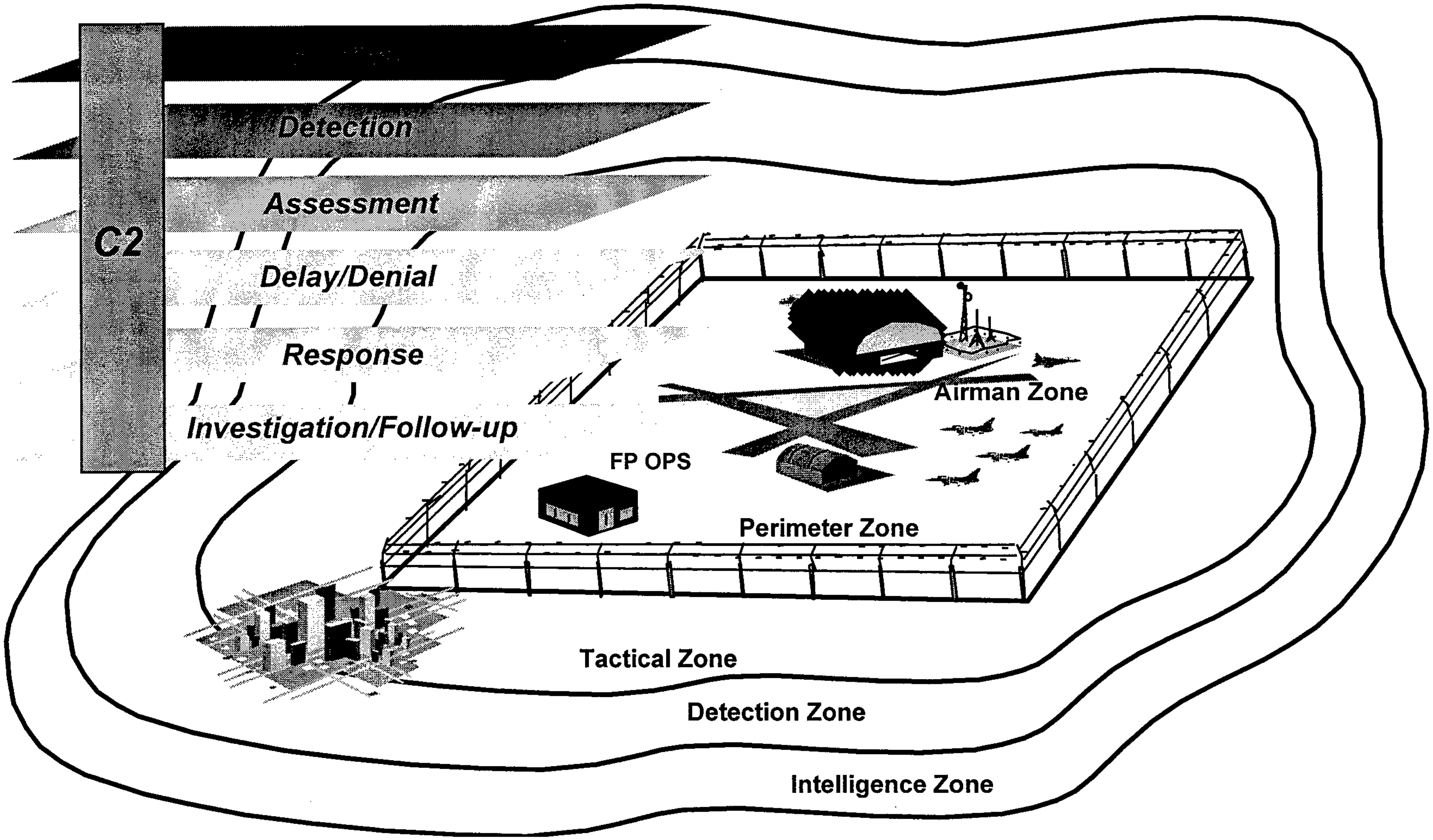
Force Protection Common Tactical Picture

Force Protection Common Tactical Picture

The Force Protection World Tactical View

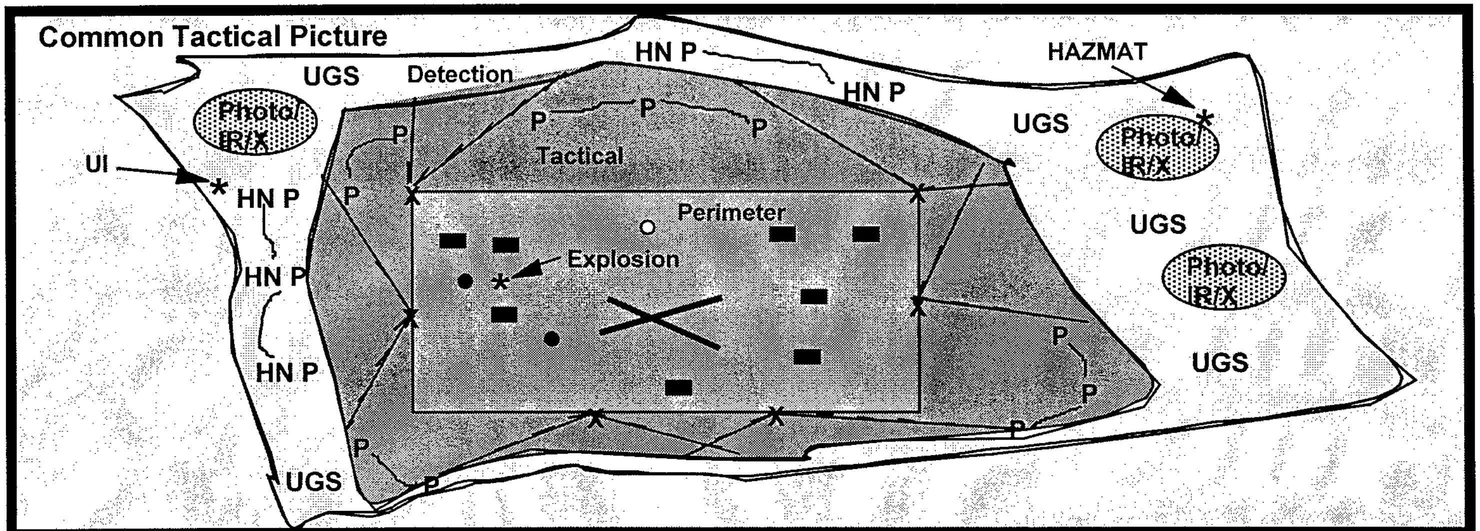
MISSION
Acquire, Deliver and *Sustain* Quality Integrated Command and Control *Systems* to Provide Force Protection to Warfighting Resources and to Government Agencies During Emergencies and Natural Disasters.

VISION
World Class Leader in Applying Technology to Force Protection C^2 Systems for the *Safety, Security* and *Survivability* of US Warfighting Assets, US *Warfighters* and Dependents Worldwide.

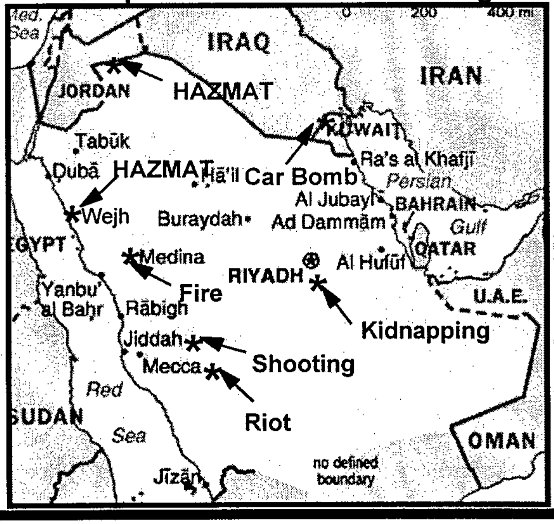


Force Protection
Common Operational Picture/Common Tactical Picture (COP/CTP)

Common Tactical Picture



Common Operational Picture – Intelligence

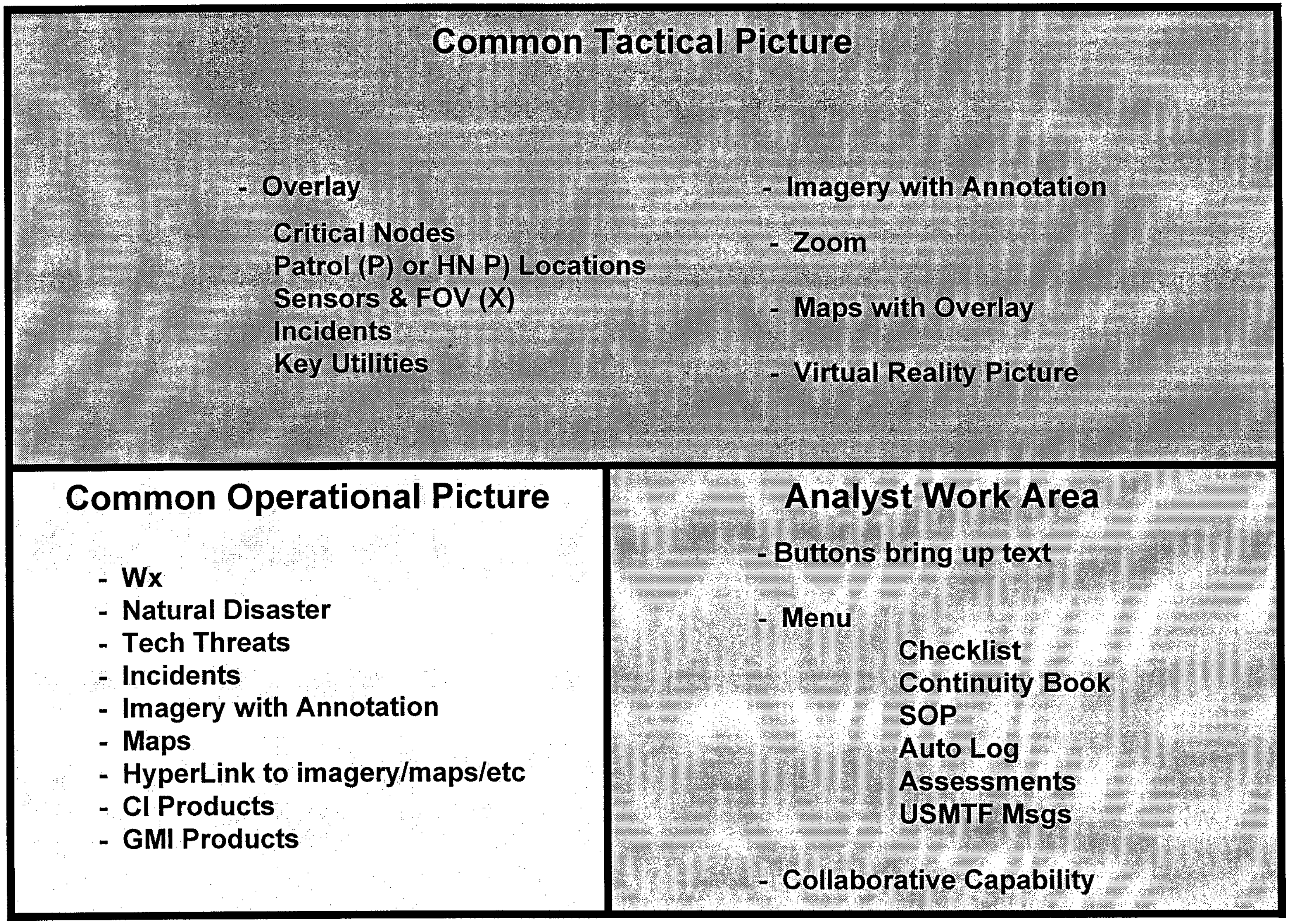


Analyst Workspace

DEFCON 5 □4 3 2 1 THREATCON N □A B C D

STATUS	
SENSORS	G Y ●
PATROLS	G Y ●
COMMS	G Y ●
UTILITIES	G Y ●
HOST N	G Y ●

THREAT	
CI	G Y ●
INTEL	G Y ●
HAZMAT	G Y ●
INFO WAR	G Y ●
INCIDENTS	G Y ●



Common Tactical Picture

- Overlay

  Critical Nodes
  Patrol (P) or HN P) Locations
  Sensors & FOV (X)
  Incidents
  Key Utilities

- Imagery with Annotation
- Zoom
- Maps with Overlay
- Virtual Reality Picture

Common Operational Picture

- Wx
- Natural Disaster
- Tech Threats
- Incidents
- Imagery with Annotation
- Maps
- HyperLink to imagery/maps/etc
- CI Products
- GMI Products

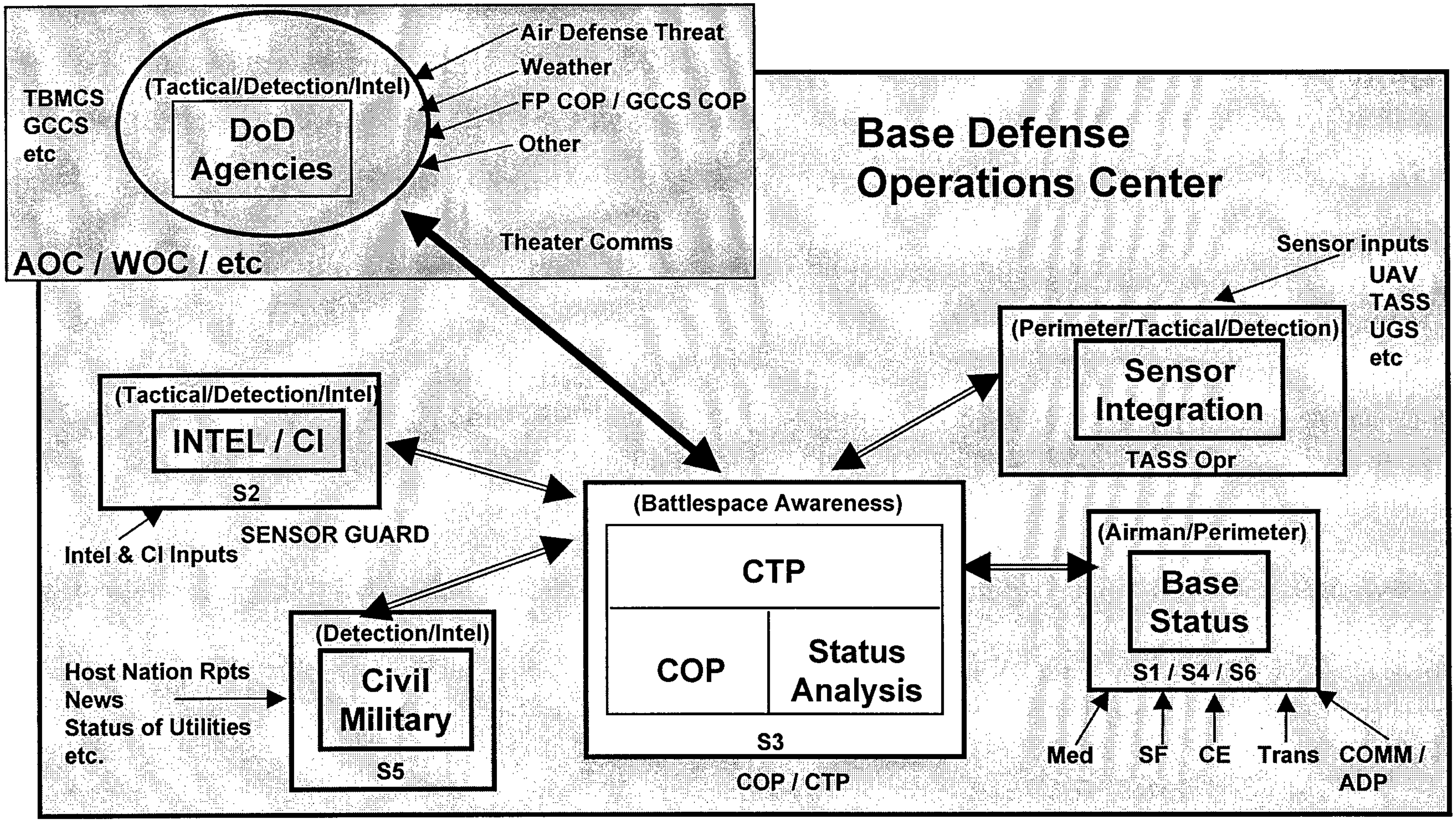
Analyst Work Area

- Buttons bring up text
- Menu

  Checklist
  Continuity Book
  SOP
  Auto Log
  Assessments
  USMTF Msgs

- Collaborative Capability

FP Battle Management C2: Unit Level



AOC / WOC / etc

TBMCS
GCCS
etc

(Tactical/Detection/Intel)
DoD Agencies

Air Defense Threat
Weather
FP COP / GCCS COP
Other

Theater Comms

Base Defense Operations Center

Sensor inputs
UAV
TASS
UGS
etc

(Perimeter/Tactical/Detection)
Sensor Integration
TASS Opr

(Tactical/Detection/Intel)
INTEL / CI
S2

Intel & CI Inputs

SENSOR GUARD

(Battlespace Awareness)
CTP
COP
Status Analysis
S3

COP / CTP

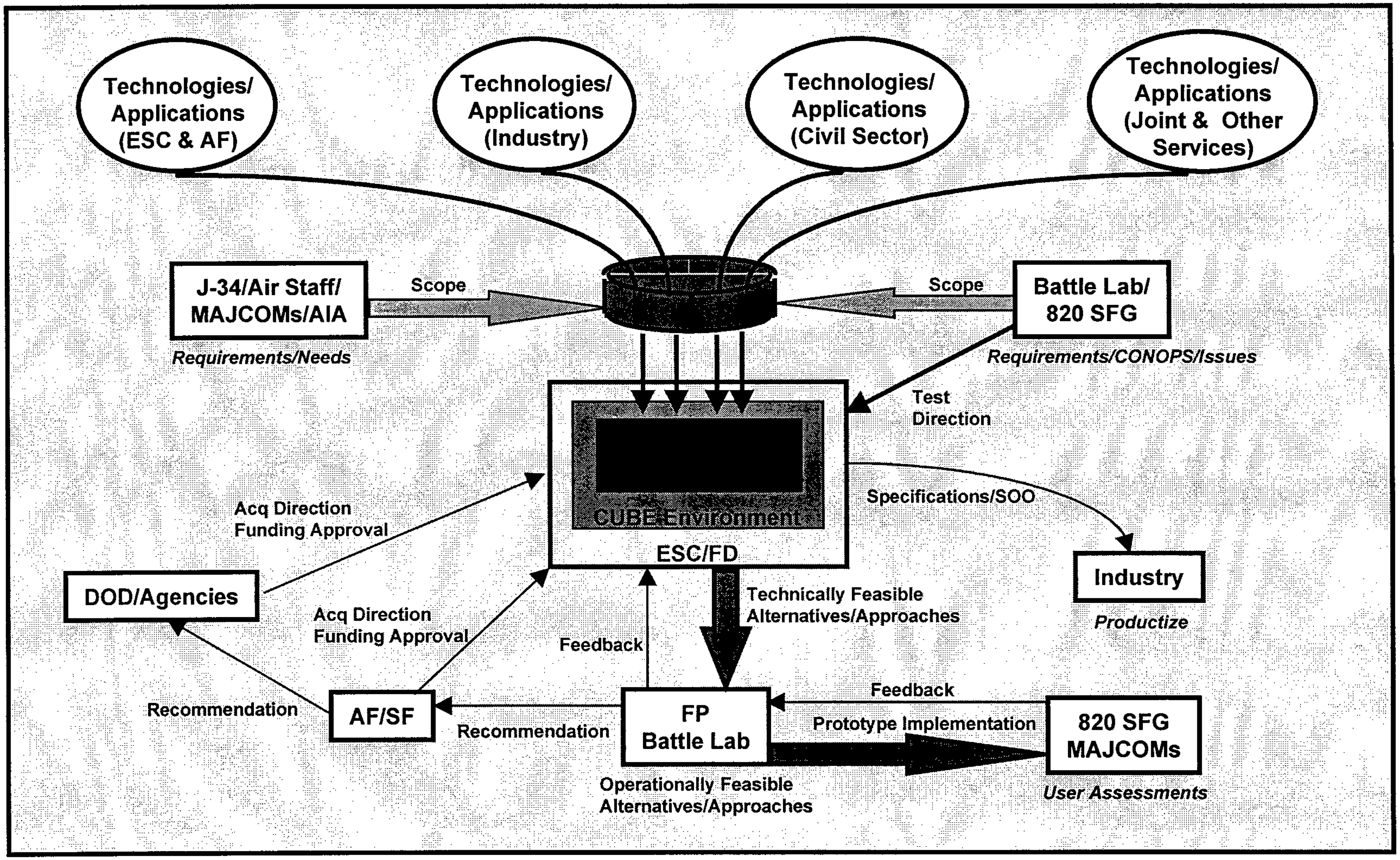
(Airman/Perimeter)
Base Status
S1 / S4 / S6

Med
SF
CE
Trans
COMM / ADP

Host Nation Rpts
News
Status of Utilities
etc.

(Detection/Intel)
Civil Military
S5

Force Protection Testbed Process


Technologies/ Applications (ESC & AF)
Technologies/ Applications (Industry)
Technologies/ Applications (Civil Sector)
Technologies/ Applications (Joint & Other Services)
J-34/Air Staff/ MAJCOMs/AIA
Scope
Requirements/Needs
Scope
Battle Lab/ 820 SFG
Requirements/CONOPS/Issues
Test Direction
CUBE Environment
ESC/FD
Specifications/SOO
Industry
Productize
Acq Direction Funding Approval
DOD/Agencies
Acq Direction Funding Approval
Feedback
Technically Feasible Alternatives/Approaches
Recommendation
AF/SF
Recommendation
FP Battle Lab
Feedback
Prototype Implementation
820 SFG MAJCOMs
Operationally Feasible Alternatives/Approaches
User Assessments

COP/CTP

- Phase I: Initial Integration and CTP Development
  - Mapping, Charting, & Geodesy capabilities and display tools
  - TASS input
  - Initial development of Sensor Integration Cell
- Phase II: COP Integration and Enhanced CTP
  - User feedback
  - Multi-Level Security investigation
  - JWARN integration?
  - Investigate CI interfaces/integration
  - Implement SENSOR GUARD as Intel/CI Cell
- Phase III: COP and CTP Enhancement
  - Incorporate analyst support tools
  - Integrate JWARN control of detectors
  - Integrate Vulnerability Assessment tools
  - Develop Base Status Cell capability
  - Develop Civil Military / External Cell

FORCE PROTECTION TECHNOLOGIES ADVANCEMENTS

- Cost-effective Wide Area Surveillance Systems (24 hr operations)
- Secure Wireless Communications for Command & Control Data & Video
- Cost-effective Real-time Remote Video Surveillance
- Human Presence Detection in Exterior Environments

FORCE PROTECTION TECHNOLOGIES ADVANCEMENTS

- Image Fusion Systems for Visible & Non-visible Light Cameras (e.g. IR, Thermal)
- Remote Surveillance
- Detection & Neutralization of Stand-off Launched Missiles
- Lightweight Deployable Ballistic Resistant Barriers
- Voiceless/Wearable/Secure Communication Capability for Force Protection Troops

POINTS OF CONTACT

- Dave Davis Tel: (978) 663-6600
  E-Mail: davisd@hanscom.af.mil
- Bernie Boucek Tel: (781) 377-8794
  E-Mail: boucekb@hanscom.af.mil
- Steve Cudlitz Tel: (781) 377-8848
  E-Mail: cudlitzs@hanscom.af.mil
- Morry Outwater Tel: (781) 377-8852
  E-Mail: outwaterm@hanscom.af.mil

14th ANNUAL SECURITY TECHNOLOGY SYMPOSIUM & EXHIBITION

DOD FORCE PROTECTION

NAVY

DOD PSEAG PROGRAM PRESENTATIONS

17 June 1998

Shirley A. MATTINGLY
(202) 433-9085/smatting@ncis.navy.mil

DoD Locks, Safes, Vaults, Seals & Containers RDT&E Program

10 Major Project Areas

Develop, procure, test, engineer, and provide criteria support for locks, safes, vaults, seals, containers, and related systems. Provide COTS evaluations and develop products and guidance to meet DOD operational and security requirements.

<u>Significant Accomplishments Oct 97 - Jun 98</u>

- Completed Lightweight Concrete Forced Entry (FE) test.
- Completed X-Ray Testing
- Completed Integrated Locking Device (ILD) Pull test
- Completed Seals Guide
- Wrote draft FF-S-2738 for seals

<u>Projected Accomplishments Jun 98 - Sep 98</u>

- Conduct Lightweight Concrete Explosive Test
- Finalize Seal Specification
- Produce & field Beta version of NSI CD-ROM

Shipboard Physical Security (SPS) Program

Three Major Project Areas

The SPS Program consists of integrated detection sensors, alarms, information displays, security force equipment, and procedures to provide defense in-depth against a wide range of external and internal shipboard threats

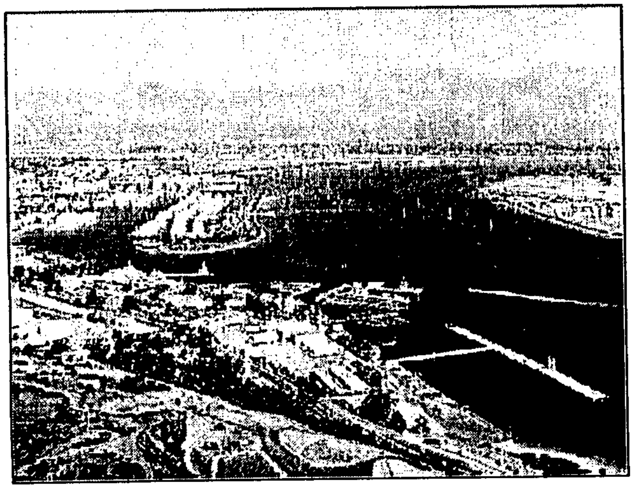
<u>Significant Accomplishments Oct 97 - Jun 98</u>

- Completed Phase I of Smart Ship Project Installation
- Completed the RF Personnel Tracking System Market Survey and Report
- Completed Smart Ship Installation Drawings
- Completed Shipboard Physical Security Mockup Facility
- Completed Phase II Smart Ship Project installation: Upgraded to Windows NT, provided man overboard reporting

<u>Projected Significant Accomplishments Jun 98- Sep 98</u>

- Develop minimum Security System Configuration for each ship class
- Develop Portable Emergency Security Force Equipment
- Test and Integrate Emerging Technologies:
    - Ship Lighting Systems
    - Infrared Lighting
    - Portable & Fixed Lighting
    - Light Intensified Cameras
    - Video Motion Detection Shipboard Applications
    - Distress Signal Feasibility Study
    - Develop DL Circuit Panel replacements

Waterfront Security



Three Major Project Areas

The Space and Naval Warfare Systems Center (SPAWARSYSCEN), San Diego is the Center of Excellence for waterfront security. SPAWARSYSCEN San Diego is responsible for fixed and transportable waterside security systems, swimmer detection sonars, and commercial off-the-shelf (COTS) equipment test and evaluation which focuses on waterfront force protection.

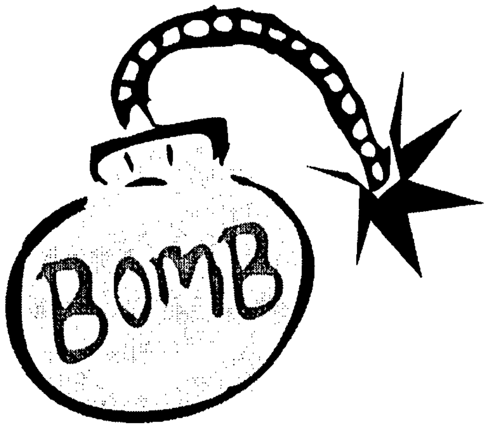
Significant Accomplishments Oct 97 - Jun 98

- Supported three installation sites: SUBASE Bangor, SUBASE Kings Bay, and ASU Bahrain
- Assisted SUBASE Kings Bay by addressing solutions to counter subsurface threats
- Coordinated with Coast Guard in identifying WSS equipment for San Diego Port
- Completed development of new Radar Track Processor and installed at SUBASE Bangor for T&E
- Completed testing of C3D upgrade w/PC based architecture.
- Conducted site survey at Portsmouth NSY for a WSS installation

Projected Accomplishments Jun 98- Sep 98

- Validate transportable system at an operational site
- Work with Smart Base for a WSS install at Portsmouth NSY
- Conduct a Site Survey within the Commander, Fifth Fleet AOR for a fixed WSS
- Upgrade SUBASE Kings Bay C3D element with a PC based replacement
- Consolidate program management of WSS and SPS

Explosive Detection Equipment (EDE) Program



Two Major Project Areas

Conduct market surveys and investigations to determine capability of COTS technology. Conduct T&E of COTS to verify performance parameters. Act as the DoD Center of Expertise for guidance on purchase and procurement of EDE. Coordinate with other federal agencies in the conduct of RDT&E efforts to meet DoD requirements.

Significant Accomplishments Oct 97 - Jun 98

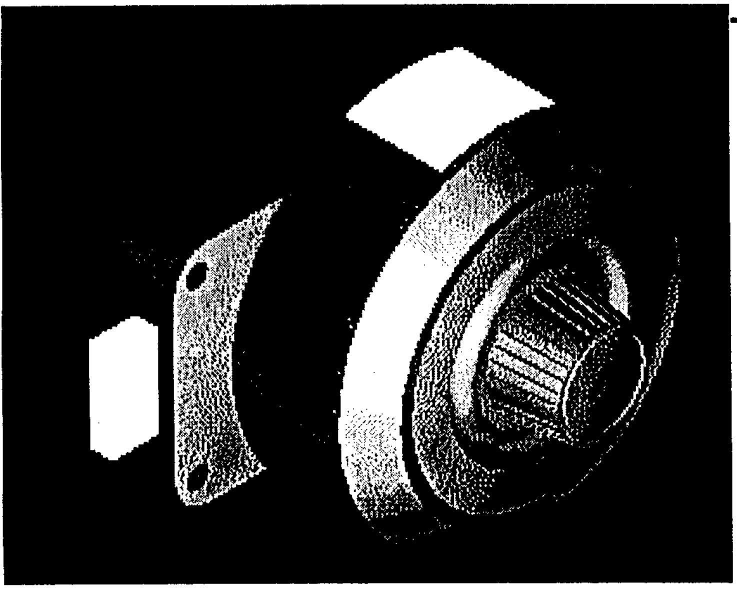
- Submitted Draft JSOR to PSEAG
- Wrote White Paper on the detection of explosives in trucks carrying concrete
- Conducted evaluation of CDS 2002, MobilSearch, remote sensing devise
- Conducted EDE Market Survey

Projected Accomplishments Jun 98 - Sep 98

- Publish EDE Six-Year Plan
- Complete EDE JSOR
- Write Concept of Operation for MobilSearch
- Conduct an Market Survey and write a report
- Write and publish a Health and Safety Guidance Document

Security Technology Project

DOD Lock Program



The objective of the Security Technology Project (STP) is to execute Congressional direction to REPLACE combination locks on secure storage spaces and GSA approved Security Containers with locks meeting Federal Specification FF-L-2740. The STP supports procurement actions, provides user training, publishes technical information, analyzes potential vulnerabilities in current products and evaluates emerging technology that could be used to improve protection of classified information

Significant Accomplishments Oct 97- Jun 98

- Developed & Distributed Weekly Data Base Reports
- Provided STP Training at 3 DoD Locations
- Supported Hundreds of "*Hotline*" Calls Monthly
- Supported *OSD, DLA, DISC & OPNAV* Requirements
- Established "*Red Label* Drawer Head Exchange Program
- Published *Security Facts!* Newsletter
- Established Web Site, *locks.nfesc.navy.mil*

Projected Accomplishments Jun 98 -Sep 98

- Conduct Follow-on Vulnerability Study
- Update & Expand Training Course (to include "teaming " with IMD)
- Identify & Analyze Candidate Information Security Protection Systems / Components
- Publish Tech Data Sheet(s) on Technical Updates
- Begin STP Program phase-out

NDIA 14th Annual Security Technology Symposium
"New Dimensions in Security Threats & Countermeasures"
June 17, 1998

Introduction

I am very pleased to be here today and to have this opportunity to tell you about some steps the FBI is taking to address critical infrastructure protection. I also commend the National Defense Industrial Association for holding this symposium, which brings together representatives from government and the private sector and contributes to our dialogue on this extremely important subject.

Three-sentence summary

There are three points that I would like to elaborate on today:

First, the domestic infrastructure is at risk as never before. Today's environment presents new threats, new vulnerabilities, and new challenges that must be confronted. Failure to address them can have enormous adverse effects, both for industry and for the economy.

Second, government and industry are finding new ways to jointly address infrastructure threats and vulnerabilities. Unlike in the past, when national security was largely a government responsibility, today the responsibility has to be a shared one, with the private sector taking on an increasingly important role.

Third, the National Infrastructure Protection Center is a new FBI organization for protecting the domestic infrastructure. At the FBI we believe that the way to address infrastructure protection is through partnerships with the private sector. We need a two-way street for the flow of information between government and the private sector. The NIPC is designed to do just that.

The Networked infrastructure

Not so long ago, there was little risk of a large-scale infrastructure disruption. Until recently, only a rare and isolated occurrence, such as an earthquake or tornado or an accidental power outage could knock out a critical service over a broad area. The physical breadth of the infrastructures made it difficult for any person or thing to cause more than an isolated and transient disturbance. And physical security measures adopted to prevent theft or vandalism generally also kept out those who might try to do more serious damage. We were able to build strong fences and be fairly sure that we were protected not only against thieves and vandals, but also terrorists and anarchists. And we took comfort in knowing that the large size of our country and its geographic separation from other countries made it difficult for foreign adversaries to launch a widespread attack on our infrastructure.

Today things are dramatically different. For while information technology can increase efficiency and productivity, and can give a nation a competitive advantage, dependence on information systems can create new vulnerabilities. Leadership in information technology is one of the things that give the United States a competitive advantage in the global economy. But it also opens us up to new types of harm that can undermine the national economy and our national security.

The infrastructure is at risk

I don't think I have to convince this audience of the need to protect the electronic networks of the domestic infrastructure.

In the past few years our society has moved on-line. Computers have found more application in our lives than one can list. Millions of cyber-citizens use Local Area Networks, the Internet, and the banking networks. No longer only for the technological elite, network technology is now accessible to the masses. We are truly a networked society.

In addition, telecommunications is now a truly global enterprise. Satellite communications, the Internet, and foreign ownership of telecommunications carriers in the U.S. have all combined to undermine the idea of a "national" information infrastructure. This means that geographic separation no longer helps fend off foreign adversaries. Now a laptop computer and a telephone connection can make it as easy to break into an infrastructure's control network from St. Petersburg, Russia, as from St. Petersburg, Florida.

Other dynamics are at work in the marketplace. There is a move towards open system architectures and commercial off-the-shelf technology. High-tech companies are rushing new products to market without a complete understanding of their security vulnerabilities. And in the many sectors, software development is concentrated in a few specialized companies. As a result, there is an increased chance that a fault can have a widespread impact.

At the same time, changes in the business environment are occurring in all sectors of the infrastructure. Deregulation, downsizing, increasing competition with new entrants into infrastructure markets, and outsourcing of core functions are some of the factors that together are putting new stress on security processes and can cause new vulnerabilities.

A third reason that the infrastructure is at risk is the increasingly sophisticated threat.

In the physical world, the range of people or groups that would have the means and motive to cause widespread destruction of an infrastructure is relatively limited – terrorist groups and hostile nations are the most likely actors. But the accessibility of the information infrastructure, global connectivity, and the rapid growth of a computer-literate population combine with the result that the means to conduct a cyber attack can be in the hands of a frighteningly large number of people.

Perhaps the greatest threat today comes from insiders. Insiders have the advantage of not needing to break into computer systems from the outside, but only to use – or abuse – their legitimate access. These individuals often have intimate knowledge of where the most sensitive information is stored, how to access the information, and how to steal or damage the data. They can make attractive exploitation targets for hostile agents. The greatest insider risk may not be your own employees. It could be the insiders or your hardware of software vendor, or insiders associated with other infrastructures like telecommunications who could target your sector.

Recreational hackers are also increasingly dangerous, in part because of the widespread availability of "cracking" tools on hacker websites. One no longer needs to have an advanced understanding of computers and the Internet to successfully crack into a company's systems. Rather, one needs only to download sophisticated hacking tools from the Internet, then "point and click" to launch an attack on any number of target sites. The results of these cyberspace joyrides could be widespread and severe, regardless of the intent.

Consider this real-world incident:

In March of last year, a teenager hacked into the local telephone company in Worcester, Massachusetts, shutting down phone service to the area's airport control tower and approximately 600 customers for over six hours. He broke into the telephone system using a common personal computer equipped with a modem. The main control tower at the airport was unable to communicate with the airport fire department or other services. The airport's main radio transmitter and a circuit which enables aircraft to send an electrical signal to activate the runway lights on approach were not operational. According to prosecutors, the juvenile was unaware of the seriousness of his actions.

If a teenager can do this for kicks, imagine what a coordinated, focused attack on infrastructure information networks could do. To date, the United States has not experienced this sort of attack, but it is not hard to extrapolate from intrusions we have seen. This is a possibility we must try to prevent from ever becoming reality.

In addition, we expect foreign intelligence services and hostile nations to increasingly use cyber tools to conduct espionage or engage in "information warfare" against us. Because no nation or group hostile to the United States can match us in traditional military firepower, none would be likely to take us on in a frontal attack. Rather, they would hit us where we are most vulnerable. And one of those vulnerabilities is our reliance on information technologies for command and control of our national security activities as well as for the daily functioning of our privately owned critical infrastructures.

Vision for the Future

What, then, is to be done? How can we protect our critical infrastructures in such a dynamic environment? The answer, I believe, lies in dialogue – dialogue between industry and the government, as well as dialogue with our international partners, to jointly identify and address the real threats and actual vulnerabilities.

Some mechanisms already exist between the government and industry for jointly dealing with computer security incidents:

The Suspicious Activity Reporting System is one example. Suspicious Activity Reports are used by financial institutions to report potentially fraudulent activity associated with electronic financial transactions. Reportable activities are defined by statute, which also specifies the measures to be taken to protect the information that is collected.

The ANSIR program is another. ANSIR stands for Awareness of National Security Issues and Response. This FBI program is designed to provide unclassified national security threat and warning information to U.S. corporations, law enforcement agencies, and other government organizations. Information is disseminated nationwide via e-mail and fax through the fifty-six FBI field offices. All told, ANSIR has the capacity to reach over 100,000 addressees.

These important programs, however, are somewhat limited in what they set out to do in the context of protecting the infrastructure. In practice, each provides for information flow that is primarily in one direction. Our vision is to build a two-way street for the flow of intelligence information and incident data between the government and industry. The government, with access to national intelligence and law enforcement information, can develop a threat picture that no one in the private sector could develop on their own. We'd like to share this with the industry. At the same time, we'd like to learn from the industry about the intrusion attempts and vulnerabilities they are experiencing. This will help us paint the threat picture more completely, and will give us a head start on preventing or disabling a nascent attack. I believe this two-way dialogue is the best way to deal with our common concern about security.

Two-way dialogue is also important with our international partners, which include foreign governments and law enforcement agencies. The benefits of such dialogue are clear, as demonstrated during a recent investigation known as Solar Sunrise, in which U.S. and Israeli authorities cooperated to identify and apprehend a group of hackers who were penetrating U.S. defense networks.

Of course, we would need to establish the parameters of the relationship. The information needs to be timely. We need clear limits on what is to be shared – limits that are both legal and equitable to both parties. And we need to make sure the information that is shared is protected. But now is the time to start building this relationship.

Impediments

If cooperation between government and industry is needed to squarely address a problem of such import, why don't we just get on with it? Well, actually it is not quite that easy. There are impediments to cooperation – sometimes real, sometimes perceived – on both sides. Let me describe a few as I understand them.

First of all, industry has historically addressed its own security challenges very effectively. It is hard to argue with decades of success. But the vulnerability and threat environment has changed dramatically in recent years. Networks have become too integrated for this independent approach. Your vulnerabilities are to a large extent my vulnerabilities, and vice versa. An infrastructure sector can't solve network security problems in isolation.

Fear of adverse publicity can also be an impediment. For a corporate leader to talk about infrastructure vulnerabilities is to invite questions of reliability and potential erosion of customer confidence. I understand the desire to keep this kind of information to yourself. But I can tell you that we at the FBI are committed to preserving the confidentiality of proprietary data during investigations and prosecutions to the full extent possible under the law. And keep in mind that a serious security incident could also have an adverse effect on customer confidence.

The competitive environment might also be seen as impediments to information exchange. If managing network risk involves dialogue and cooperation among competitors, both the natural forces of the marketplace can put a damper on cooperation. But there are ways of sharing without losing competitive advantage or running afoul of regulators. The Network Security Information Exchange forums established by the government and the telecommunications industry are probably the best example of the benefits of a controlled dialogue on infrastructure vulnerabilities. These forums bring together the major players of the telecom industry, the intelligence community, the FBI, and other government agencies to address network security. They have been operating successfully for years. Nondisclosure agreements, strict control over participation, and strong commitments to respect the confidentiality of data go a long way towards allowing competitors and the government to cooperate.

And there is the question of costs and benefits. "What's in it for me?" is a fair question for the industry to ask. I understand a reluctance to share incident and vulnerability information with the Federal Government if the cost of reporting outweighs the benefit received in return. But I can tell you that the FBI is committed to the idea of a two-way street for the flow of information between government and industry. We know we have to add value if we want a partnership to work.

From the government's perspective, protecting sources and methods is always a chief concern when disseminating intelligence information. By its nature, this information has to be handled carefully so as not to compromise the government's sources and collection methods. Access to classified material requires a government-issued security clearance and a legitimate need to know. With the right ground rules, though, we can make classified information available, and we are committed to doing so.

Also when dealing with a criminal investigation, law enforcement authorities must be concerned about rules of criminal procedure so as not to jeopardize the prosecution of the case. Specific rules prohibit sharing of certain information, such as grand jury information, and this can affect how information is handled. But we have learned that there are ways to sanitize the data while still providing a tremendous amount of useful information for the private sector.

The way ahead

None of these impediments needs to prevent dialogue. We believe this, and I'd like to tell you about two ways we are acting on this belief.

NIPC

In February of this year, the FBI created the National Infrastructure Protection Center, or NIPC. The NIPC's mission is to detect, deter, prevent, assess, warn, respond to, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target our critical infrastructures. Notice the emphasis on prevention. Our job is not simply to investigate and respond to attacks after they occur, but to learn about them beforehand and prevent them. This requires collecting and analyzing information from all available sources, and disseminating analyses and warnings of possible attacks to potential victims, whether in the government or private sector.

This broader mission is something that the FBI cannot do alone. It requires the combined efforts of many different government agencies. The Departments of Defense, Treasury, Energy, and Transportation and others have significant roles.

We also need the involvement of State governments because they own, operate, or have jurisdiction over some of the critical infrastructures and because their agencies are often the first responders in the event of a crisis.

And, perhaps most importantly, this mission requires the intensive involvement of the private sector. Private industry owns and operates most of the infrastructures and has the greatest expertise understanding of the technical problems and solutions. Industry also has the only direct knowledge of the real-world intrusions they are experiencing. Individual security incidents at network control centers across the industry could be part of a larger coordinated attack. Who can put the pieces together if no one says anything? We simply must ask the private sector to be involved with infrastructure defense.

Recognizing the roles of all these players, the NIPC is designed on the notion of a partnership. Partnership begins with inclusive representation, and the NIPC is being staffed with representatives from the other critical federal agencies, from State and local law enforcement, and from private industry, in addition to the FBI. This will foster the sharing of information and expertise, and improve coordination in the event of a crisis. And we will augment the physical presence of these representatives by establishing electronic connectivity to the many different entities in government and industry who might have, or need, information about threats to our infrastructures.

When fully staffed, the FBI will have 23 Special Agents at the NIPC, complemented by 76 Special Agents serving on Computer Investigation and Infrastructure Threat Assessment teams in each of the FBI's Field Offices. The NIPC will also have personnel from other government agencies and the private sector, for a total in-house staff numbering 125. This team will carry out the NIPC mission of analysis, warning, investigation, outreach, and coordination.

We have a lot of work to do in order to build the trusted relationships we need with your industry and the other infrastructure sectors. This will take time. But we are committed to this process, and we are looking forward to working with the private sector in a true win-win partnership.

InfraGard

A second example of our commitment to two-way partnership is InfraGard, a pilot project sponsored by the FBI's Cleveland Field Office. The name "InfraGard" refers to "guarding the information infrastructure." The program is a cooperative effort in the exchange of information between the business community, academic institutions, the FBI, and other government agencies to protect the information infrastructure.

InfraGard features an alert network that members can use to report intrusions. Reports are sent to the FBI via encrypted e-mail in two forms: a detailed description and a sanitized description. The FBI uses the detailed description to analyze the incident, identify trends, and open an investigation if warranted.

However, only the sanitized version is shared with other InfraGard members. The beauty of this procedure is that the reporting organization can choose the words to describe the intrusion to their competitors.

InfraGard also features a secure website that members can use to obtain information about recent intrusions and infrastructure protection efforts, access original research on security issues, and confer with other members. The program also offers seminars and training to educate members on how they can prevent and respond to infrastructure attacks.

InfraGard membership is large and diverse. Currently the Cleveland InfraGard has approximately fifty-six member organizations, including KeyCorp, the Federal Reserve, TRW, Ameritech, Case Western Reserve University, and many government agencies such as FAA, NASA, and city and county agencies. Potential members must sign a membership agreement and a confidentiality pledge. And they must make a commitment to actively participate.

InfraGard is an experiment. We have high hopes that InfraGard will prove successful, and if it does we plan to move to a national system on the same model which would be managed by the NIPC.

Conclusion

In conclusion, I'd like to stress that the electronic infrastructure of the United States is at risk today as never before. This infrastructure is a critical national resource.

It is at risk because of new vulnerabilities, changes in the business environment, and the emergence of increasingly sophisticated threats.

I believe that the government and the private sector have security interests in common. But neither can address these security interests alone. The National Infrastructure Protection Center and InfraGard are two concrete steps we at the FBI are taking to build partnerships with the private sector to prevent and manage increasingly serious threats to critical United States infrastructures.

Let us get on with it. Let us – government and industry – join forces to defend against the Information Age threats that can disable our critical infrastructures. Let us not wait any longer.

Interested U.S. corporations should provide their email address, position, company name and address as well as telephone and fax numbers to the national ANSIR Email address at ansir@leo.gov. Individual ANSIR Coordinators in the respective field divisions will verify contact with each prospective recipient of ANSIR Email advisories.

COMMERCIAL OFF-THE-SHELF EQUIPMENT WORKING GROUP

Presented By:
Mr.. William J. Witter
Defense Special Weapons Agency
Alexandria, VA

CWG Mission

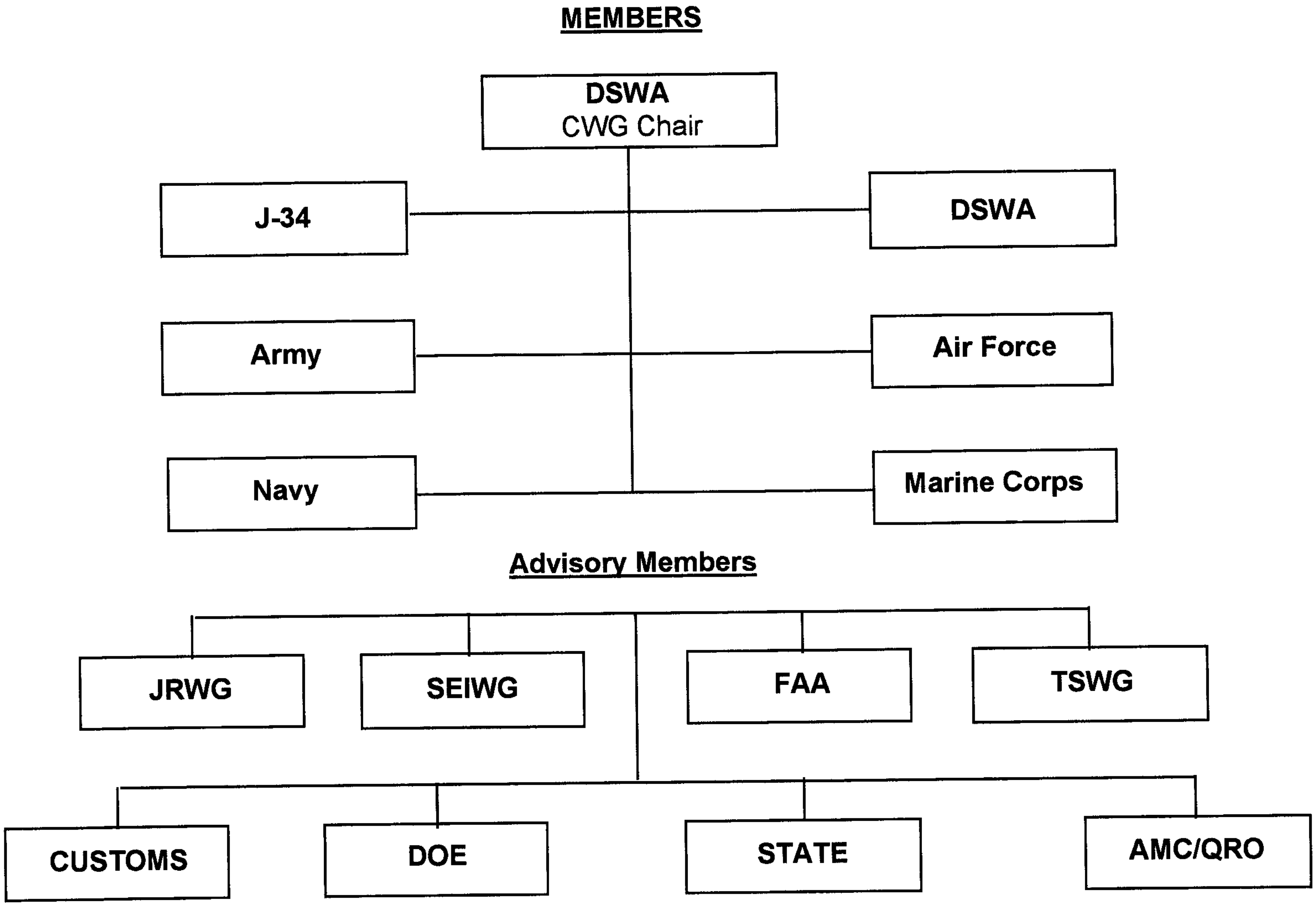
PSEAG

\

CWG

To support the DoD PSEAG through identification and rapid procurement of COTS items for test and evaluation by Services and DSWA for use as material solutions to Service, CINC, and field commands, in response to identified antiterrorism and Force Protection (AT/FP) deficiencies as provided and prioritized by J-34.

CWG Organization



MEMBERS

DSWA
CWG Chair

J-34

DSWA

Army

Air Force

Navy

Marine Corps

Advisory Members

JRWG

SEIWG

FAA

TSWG

CUSTOMS

DOE

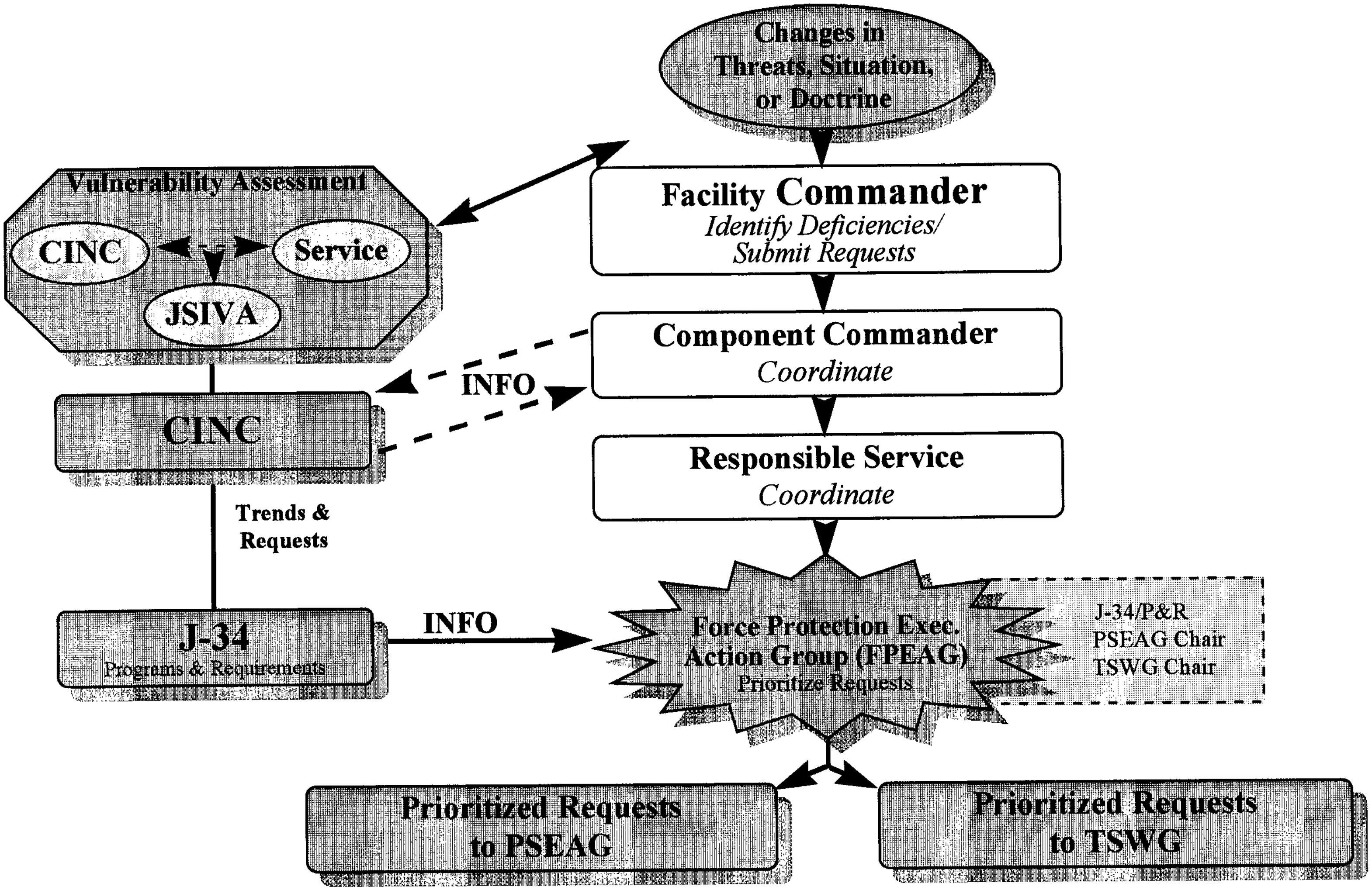
STATE

AMC/QRO

Major Responsibilities

- COMMITTEE
  - Market Surveillance of Commercial Products
  - Task Services / Agencies to Conduct and Report Evaluations
  - Review and Approve Evaluation Plans and Reports
- SERVICES / AGENCIES
  - Prepare Evaluation Plans and Reports
  - Conduct Field and / or Laboratory Evaluations

The Request Process



Changes in Threats, Situation, or Doctrine

Facility Commander
Identify Deficiencies/ Submit Requests

Component Commander
Coordinate

Responsible Service
Coordinate

Force Protection Exec. Action Group (FPEAG)
Prioritize Requests

J-34/P&R
PSEAG Chair
TSWG Chair

Prioritized Requests to PSEAG

Prioritized Requests to TSWG

Vulnerability Assessment
CINC
Service
JSIVA

CINC

INFO

Trends & Requests

J-34
Programs & Requirements

INFO

CWG Priorities

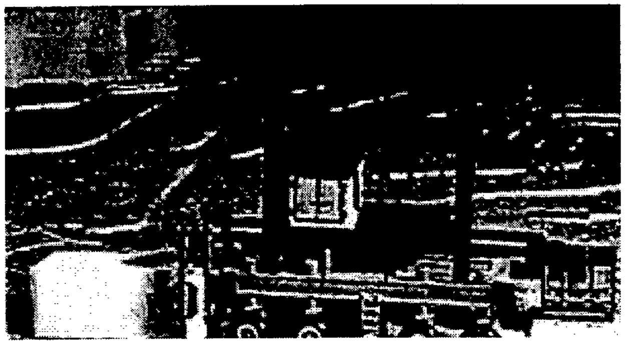
- 1. Personnel Alerting Systems (Army)
- 2. Explosive Detection Devices (Navy)
  - a. Equipment priority- handheld, static, under water
  - b. Size priority: car, mail, individually carried
  - c. Explosive priority: C4, Semtex, Nitroglycerin, Sodium Chloride, TNT, RDX
- 3. Explosive Mitigation (Army, Navy, & DSWA)
  - a. Blast containment
  - b. Equipment reducing required standoff distance
  - c. Equipment providing safe areas
- 4 . Personal Protection Equipment (Army)
  - a. Chemical / biological protective equipment
  - b. Protective vests
  - c. Flares
  - d. Mace
- 5. Ground Sensors (Army & Air Force)

CWG Priorities

- 6. Active Barriers (Air Force)
- 7. Passive Barriers (Army & Navy)
  - a. Portable
  - b. Fixed
- 8. Thermal Imaging Devices (Air Force)
- 9. Wide Area Security & Surveillance System (Army & Air Force)
  - a. Thermal based systems
  - b. Harbor / shipboard
  - c. Underwater
- 10. Under Vehicle Surveillance Systems (Army & Air Force)

Photoneutron Probe Explosive & Nuclear Material Detector

Supporting Major Program Title: Advanced Security Concepts



Description/Objective

- Permits Portable Non-Intrusive Inspection of Vehicles and Containers
- Combines X-Ray ID of Suspicious Shapes with Neutron Probe for Detection of Specific Contraband
- Integration Permits Quick Scan then Slow Meticulous Inspection for Drugs, Explosives, or Nuclear Material

Significant Accomplishments - FY 98 (Oct 97-May 98)

- Contract awarded to ARACOR, Jan 98

Projected Accomplishments - FY 98 - 99

- **FY 98 (Jun 98 –Sep 98)**
- Develop Conceptual System Design
- Estimate of Contraband Detection Capabilities in Various Operating Scenarios
- Laboratory demonstration of Beryllium plate

FY 99 (Oct 98 - Sep 99)

- Prototype Demo

Agency: HQ/DSWA
Point of Contact: Mr. Witter
Phone Number: (703) 325-1002 DSN 221-1002

DEFENSE SPECIAL WEAPONS AGENCY • UNITED STATES OF AMERICA •

Current Projects

- EXPLOSIVE DETECTORS
- CCTV CAMERAS
- PERSONNEL ALERTING SYSTEM

Force Protection Program

SEMPER VIGILANS

DEFENSE PROTECTIVE SERVICE

A Defense Protective Service Briefing

Pentagon

- Large single office office building
- More than 7,000,000 sq ft
- 17.5 miles of hallways
- 25,000 employee's
- Shopping mall
- Metro subway Station

Defense Protective Services

- A Division of Washington Headquarter Services headed by Mr... David O. Cooke
- Mission: To provide a safe and secure work environment for DoD
- Performs law Enforcement and security functions

Pentagon Reservation Grounds

- **Police Patrols**
  - Patrol cars
  - Bike patrol
  - Foot patrols
- **CCTV**
- **Lighting**
- **RAM Program (Random Antiterrorist Measures)**
- **Barriers**

Pentagon Perimeter

- Access Control
- X-Ray and metal detectors
- Electronic intrusion detection and duress system
- CCTV
- Mantraps at River and Mall
- Mylar

Inside the Pentagon

- Officer Patrols
- CCTV
- Employee training for emergencies
- Response procedures
- Utility Area Controls

Special/Secure Areas

- Access control
- Electronic intrusion/detection system
- Electronic sweeps and countermeasures
- Construction Criteria
- Staff training

THREATCON PROGRAM

(Terrorist Threat Condition)

- **Measures consistent with threat against facilities**
- **Threat Assessment in accordance with DoD 0-2000.12-H**
- **Predetermined increased security measures for each level**

Response Plans

- Photo and biographies of occupants
- Video and still photos of office layout
- Environmental controls data on hand
- Perimeters (Inner/Outer) pre-established
- Officer positions pre-established
  - Police for Alarm response
  - EST for Hostage response

Emergency Services Team (EST)

- SRT Trained
- Special Weapons
- Hostage Negotiations Capable
- NBC trained and equipped
- Protective operations

NBC Response

- **10-90 Gold Response Plan published**
- **Awareness level training for all DPS personnel**
- **Operations level training**
- **Training through:**
  - Army Chemical School
  - Dept. of Energy
  - U.S. Public Health Service

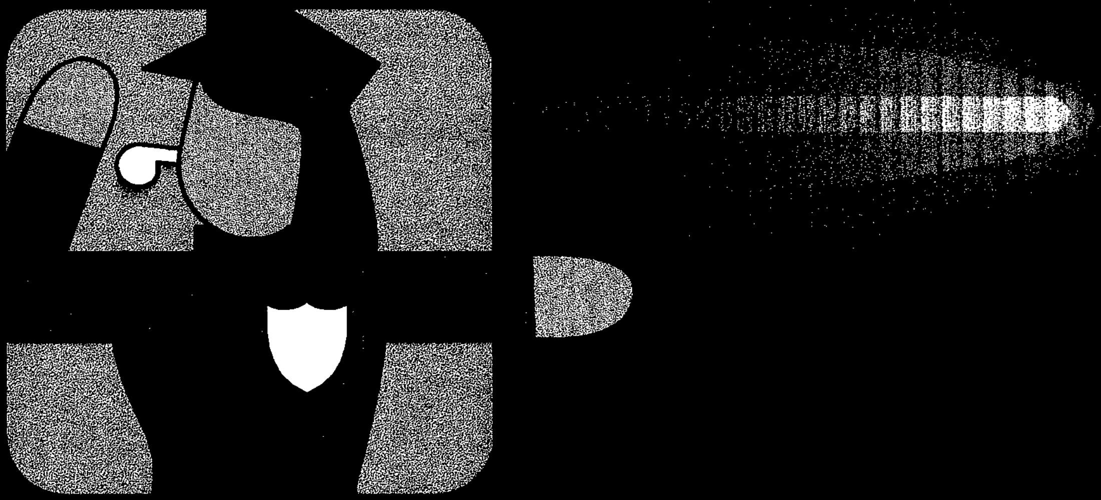
Detection Equipment

- PRM-470 detects Gamma & Neutron Radiation
- Detection equipment deployed on all Special Events, Rams, and THREATCON Levels Alpha and above

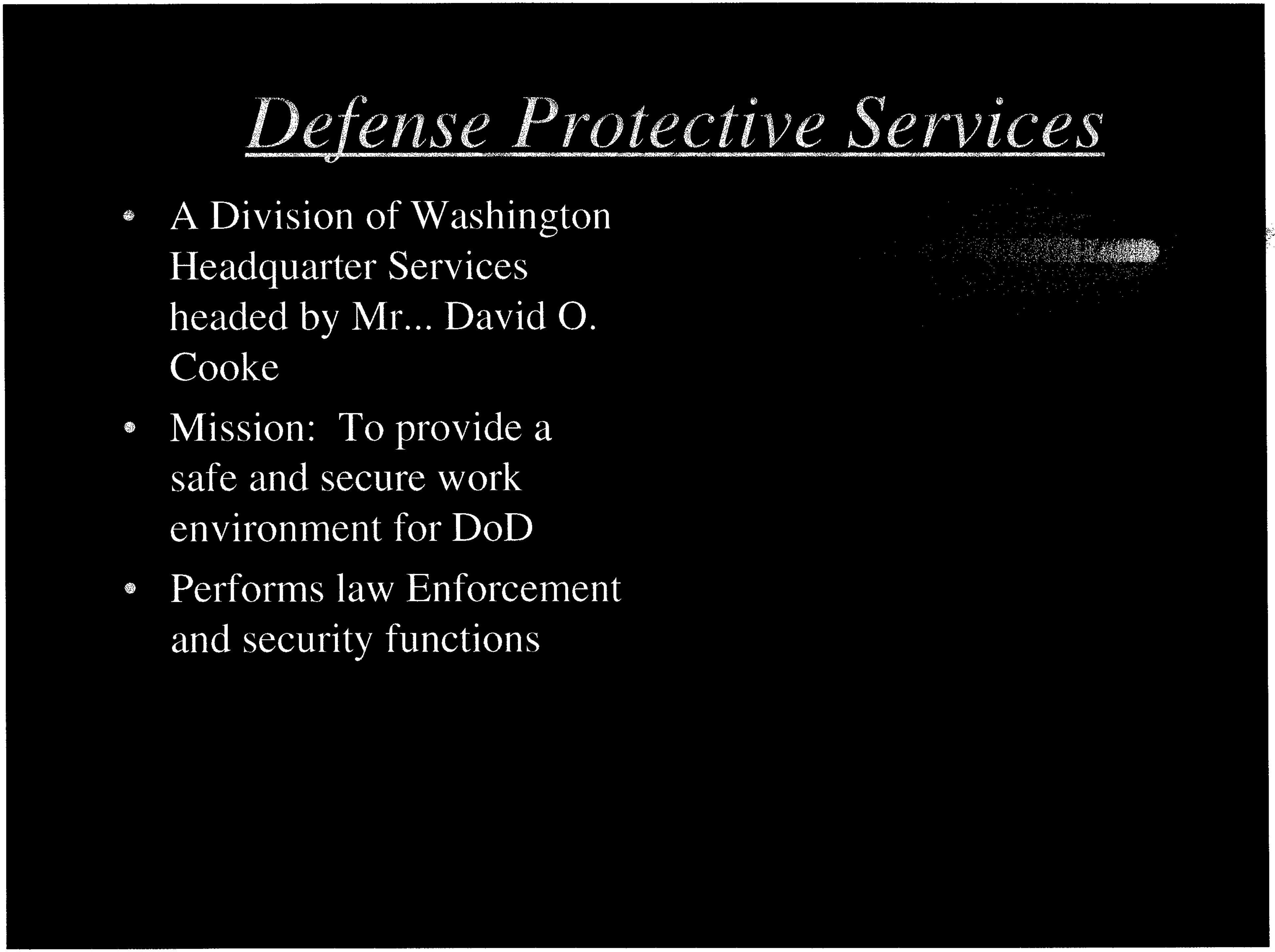
Respiratory Protection

- Escape Hoods
- Quick Masks

Force Protection Program

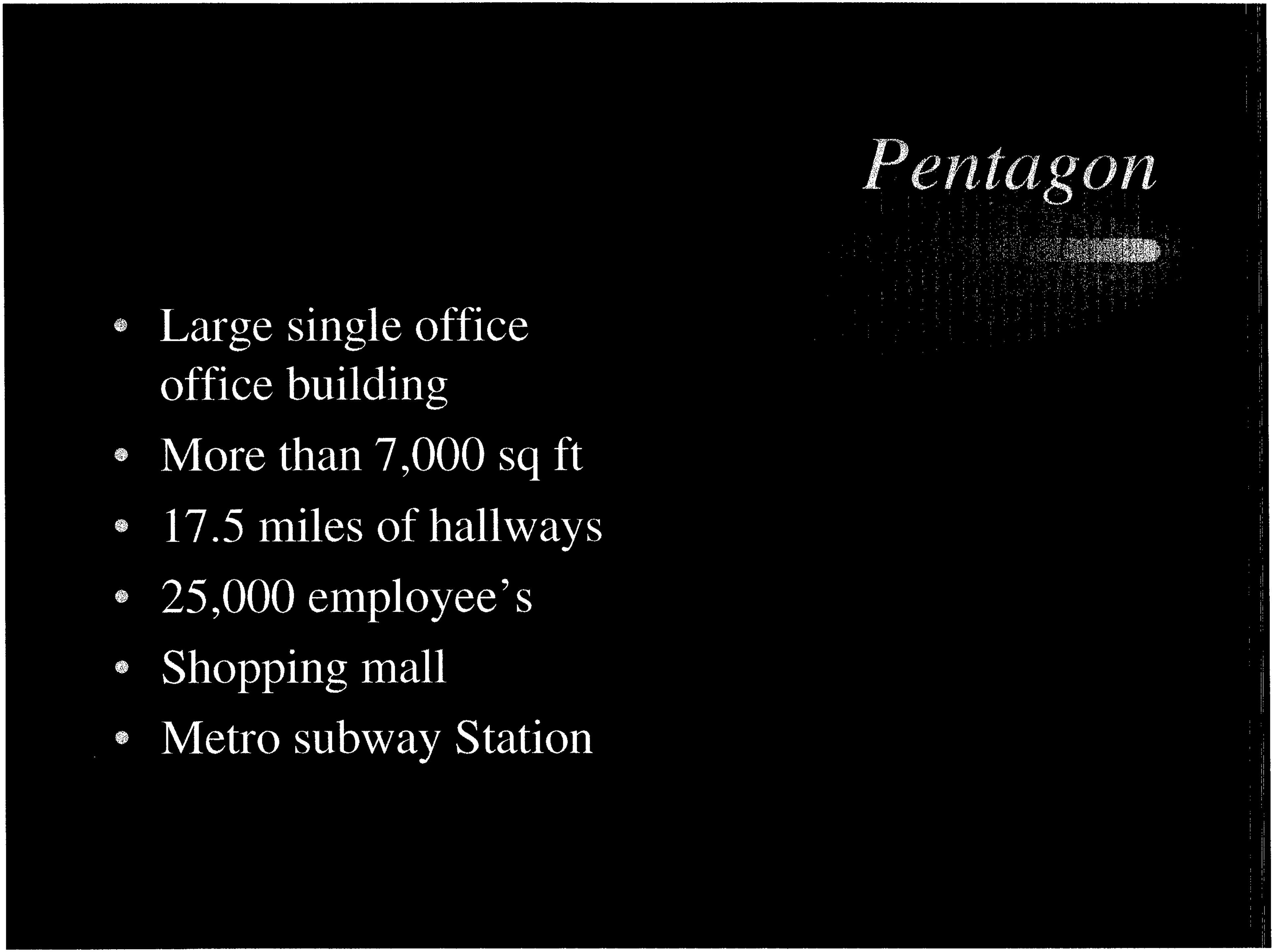


A Defense Protective Service Briefing



Defense Protective Services

- A Division of Washington Headquarter Services headed by Mr... David O. Cooke
- Mission: To provide a safe and secure work environment for DoD
- Performs law Enforcement and security functions



Pentagon

- Large single office office building
- More than 7,000 sq ft
- 17.5 miles of hallways
- 25,000 employee's
- Shopping mall
- Metro subway Station

Pentagon Reservation Grounds

- Police Patrols
  - Patrol cars
  - Bike patrol
  - Foot patrols
- CCTV
- Lighting
- RAM Program (Random Antiterrorist Measures)
- Barriers

Pentagon Perimeter

- Access Control
- X-Ray and metal detectors
- Electronic intrusion detection and duress system
- CCTV
- Mantraps at River and Mall
- Mylar

Inside the Pentagon

- Officer Patrols
- CCTV
- Employee training for emergencies
- Response procedures
- Utility Area Controls

Special/Secure Areas

- Access control
- Electronic intrusion/detection system
- Electronic sweeps and countermeasures
- Construction Criteria
- Staff training

THREATCON PROGRAM

(Terrorist Threat Condition)

- Measures consistent with threat against facilities
- Threat Assessment in accordance with DoD 0-2000.12-H
- Predetermined increased security measures for each level

- AFDW
- Coordination

Response Plans

- Photo and biographies of occupants
- Video and still photos of office layout
- Environmental controls data on hand
- Perimeters (Inner/Outer) pre-established
- Officer positions pre-established
  - Police for Alarm response
  - EST for Hostage response

Emergency Services Team (EST)

- SRT Trained
- Special Weapons
- Hostage Negotiations Capable
- NBC trained and equipped
- Protective operations

NBC Response

- 10-90 Gold Response Plan published
- Awareness level training for all DPS personnel
- Operations level training
- Training through:
  - Army Chemical School
  - Dept. of Energy
  - U.S. Public Health Service

Detection Equipment

- PRM-470 detects Gamma & Neutron Radiation
- Detection equipment deployed on all Special Events, Rams, and THREATCON Levels Alpha and above

Respiratory Protection

- Escape Hoods Provided to the SecDef, DepSec, CJCS & VCJCS and SecDef and DepSec Office staff

THOMAS J. FALVEY, COMMISSIONER
PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION
NDIA
17 June1998

- **WAITING FOR DISASTER IS A DANGEROUS STRATEGY**

Earlier this week Steve Mitchell gave you an overview of the work of the President's Commission on Critical Infrastructure Protection and the resultant Presidential Decision Directive 63, or PDD. For the next 30 minutes, I'd like to share some perspectives of infrastructure assurance and how it relates to DOT and the transportation industry.

I'd like to go over some the challenges facing DOT and the transportation industry in implementing infrastructure protection within the transportation sector. First a quick overview of the transportation sector, and a little on how DOD plays into the equation.

Of all our critical infrastructures, transportation is perhaps the most visible from a physical perspective. Through the years and through innumerable incidents, the owners and operators of transportation have learned to deal with the physical threat, from natural disasters to terrorist attacks. However, transportation now depends on information and communication systems we never see. All our modes of transportation, as well as other sectors, are increasingly becoming dependent on GPS. SCADA systems remotely monitor and operate pipelines over thousands of miles of pipe. With the ability to expand highway capacity greatly limited by any number of factors, Intelligent Transportation Systems, or ITS, are increasingly becoming critical to managing highway traffic growth.. Ships are tracked into and out of our largest ports by Coast Guard's Vessel Traffic Services, critically dependent on voice communications, radar and television monitoring systems, and computer tracking systems. Our National Airspace System is undergoing the final design phase for replacing our 25 year antiquated system. This new architecture is dependent on open system architectures, GPS, new computer based management systems, and digital communications.

In the past the business of transportation has largely been conducted with paper-based contracts and agreements, orders, letters of credit, invoices, and manifests. Today, however, the business of transportation, along with the world around us, is rapidly adapting to a virtual world. The information technology explosion is generating new ways of doing business. Transportation is becoming an information-based industry critically dependent on data and instantaneous communications. Electronic commerce and electronic data interchange, making just in time delivery the norm rather than the exception, are increasing efficiencies and giving many industries and companies a competitive edge in the global economy. Railroad companies continue to merge, consolidating operations centers and rail lines, moving more and more traffic onto fewer corridors, making these systems more vulnerable to attack. Railroads depend on extensive and interactive databases to track equipment and shipments, ensure proper billing, and ensure effective scheduling for intermodal connections. Computers have become indispensable and critical to the efficient running of our rail and mass transit systems, for operating our pipelines, and for controlling traffic flows in our cities and on our roads. Yet, at the same time, information system operation and maintenance are being outsourced, highlighted most visibly by the Y2K problem. Extensive dependencies on data bases, Supervisory Control and Data Acquisition (SCADA) and other control systems, and a customer focus allowing computer-based updates on shipments, make these systems more vulnerable to intrusion via the internet and communication lines.

The Commission found that while this nation's transportation system is robust, new information-based systems are creating new vulnerabilities that are not yet fully understood. While the industry has a long history of responding to natural disasters and other threats and keeping our transportation system running, for the most part little consideration is given to the growing vulnerability of our information-based systems. Critical transportation nodes do exist, most of which are largely recognized by the owners and operators – the challenge is how to protect those nodes during a national emergency. Greater government oversight is not the answer. I believe that given the right information, industry will take the necessary steps to protect their critical systems, and thus contribute to the security and the economic well being of the nation. DOT must act as the leader, the facilitator, and take the initiative to get critical information and share it with the owners and operators of our critical transportation infrastructure.

I spoke at a transportation conference this past year, with a major focus on use of the internet to conduct business. Not one mention was made of security considerations. We must realize that today even amateurs have access to the technological tools needed to penetrate systems and cause trouble. The Internet contains hacker sites with simple instructions on how to penetrate systems. The capability to intrude into computer systems increases with a corresponding drop in the computer skills needed to use those tools. System managers are frequently hired without adequate background checks, and in many cases maintenance of information systems are being outsourced with no security controls whatsoever. We've all heard of the Y2K problem facing this country – and I believe this is the greatest of all threats facing this country today—but how much thought is given to where the Y2K solutions are being implemented. The end result is that infrastructures are constantly in danger from people intent on penetrating or disrupting them -- all they need is a personal computer and a modem. The question that our CEO's and CIO's must ask is whether or not we're staying ahead of that trend.

In summarizing some of the findings related to the transportation sector, the Commission found the existing threat dissemination and information sharing process is relatively informal and geared to counterterrorism, not to information based threats. Except for aviation and ports, infrastructure contingency and response plans are non-existent, as are industry security standards and guidelines. Security managers, particularly on the information side, are unable to make a case for action because of a lack of credible data. While we assume the private sector knows its own critical assets, we have no process to identify those facilities that may require protection during a national emergency.

On the Defense side, Department of Defense Planning Guidance (DPG) 2000-2005 just published in April 1998 notes national guidance requires the Department to develop a plan for protecting its own critical infrastructures, implement that plan within two years, and contribute its portion of the National Infrastructure Assurance Plan. To advance the development of an assurance assessment capability, DOD Directive 5160.54 Critical Asset Assurance Program provides a framework to develop the requisite plan and provide a satisfactory level of infrastructure assurance. The Secretary of the Army is the Executive Agent for that program.

The DPG further tasks the services and most of the unified commands, including TRANSCOM, to:

- identify the critical or minimum essential infrastructure required to provide an acceptable level of service;
- develop and implement plans for the assurance of their critical infrastructures; and
- establish standing intelligence collection requirements and a threat baseline.

Just recently DOD, in Joint Vision 2010, adopted "Dominant Manuever" as a theme, meaning DOD will require rapid movement of materials, troops and supplies to any point on the globe – "just in time delivery" – from fort to foxhole. Any delay or disruption of that system will have serious impact, and therefore, we must ensure our transportation systems are secure.

Recognizing the need to closely cooperate, DOT and TRANSCOM is developing a close working relationship to ensure we leverage each others capabilities in analyzing threats and vulnerabilities to critical transportation assets, and in developing a plan to assure those assets both for national as well as economic security.

The NAS presents a serious challenge to DOT. The Federal government must take the lead in protecting critical infrastructure. The NAS is a highly visible asset that presents a tempting target to the information warriors and hackers around the world. However, the current version of the modernized NAS is vulnerable because of open system architectures, internet connectivity, an absence of backups to critical systems, a risky dependency on GPS, and a sharing of operational and administrative systems.

Speaking of GPS, the current Federal Radionavigation Plan calls for GPS to be the sole radionavigation service by 2010. Nonetheless, we see a general lack of awareness of GPS vulnerabilities, particularly to man-made and natural interference.

These open questions on the vulnerabilities of the NAS and GPS continue to lead us to one basic conclusion:

WE MUST ACT NOW TO PROTECT OUR FUTURE

To do that we must convince our leaders of the future threat without an obvious current threat.

> **The threat is largely unknown and undefined in the traditional sense. Technology is largely unavailable to detect intrusions into information systems; we have no idea of how extensive a problem we have. Hacker tools are freely available on the WWW. Thousands of viruses exist. Many critical systems have unauthorized, unprotected external modem connections. Tests have shown even well protected systems can be hacked and penetrated. If a terrorist or nation-state decided to wreck havoc on the US, a kid can be hired for a few thousand dollars to do the work and not leave a trail. Unlimited vulnerabilities with an undefined threat present unparalleled challenges to risk as well as financial managers.**

If this commission ultimately has any impact on securing our critical infrastructures, the Federal Government likely will need to take a strong leadership and coordinating role. Within the transportation sector, DOT must take that role -- not armed with a regulatory solution, but as a coordinator and facilitator, as a leader. Industry and DOT must come together and develop at least a basic contingency plan on how to respond to a threat or an attack on our transportation systems. If DOT can get segments of the transportation industry together to address common threats and vulnerabilities, on a non-adversarial and non-attributional basis, even if DOT stays out of the room, we will be doing a great service to the nation and go a long way to preserving our national security and economy.

GOVERNMENT MUST SET THE EXAMPLE, BUT THE OWNERS AND OPERATORS ARE THE KEY TO SUCCESS

The increased risk of computer crime has led to the Attorney General's announcement of the start-up of the FBI's National Infrastructure Protection Center well before the final signing of the PDD. Almost concurrently the press reported several cases of criminal hacking into sensitive systems, in particular the "Solar Sunrise" event.

We in DOT support the FBI's jumping our in front of the problem in such an aggressive fashion by establishing the NIPC. We see one of their most critical responsibilities will be rapid and concise reporting of ongoing information-based attacks. Yet, we all know establishment of the center in the FBI will not immediately solve all our computer intrusion problems. The FBI must be given time to establish an effective analysis and dissemination process. Law enforcement agents, historically trained to keep law enforcement sensitive information from public disclosure, must now be trained to share information to protect our critical systems. We, both industry and government, must press the FBI to notify Federal agencies and others of ongoing attacks on computer and other information systems. This highlights the key issue – how to balance the needs of law enforcement with the overarching need to protect our infrastructures. This issue will present a major national policy challenge in the months and years to come.

We must improve our information sharing and threat dissemination processes. We need to understand who needs what information, develop effective systems and processes to share that information, and ensure that information gets to the individual who needs to take action. We must routinely test the effectiveness of that system. We must break down the information stovepipes that now exist. And it must be a two way street. Both the private sector and the federal government may be faulted for not sharing information. We must find a way to trust each other.

Information overload also presents a significant challenge. Once we start sharing information as envisioned, how do we process the data, sort out the important data while ensuring we protect it from public disclosure and not compromising law enforcement investigations, and disseminating with sufficient confidence to take perhaps costly countermeasures.

> **Until the issue of protecting sensitive information is resolved, we must make this clear to the industry: Do not share any information with the government you would not want on the front page of the Washington Post!.**

Unfortunately, with new technologies comes new vulnerabilities, and our systems have been slow in identifying the need for reducing those vulnerabilities. Organizations may help themselves by requiring assurance provisions when they design and purchase new systems. Beyond that, both the federal government and the industry must identify their critical systems and increase efforts to conduct R&D to protect those systems. Security guidelines or standards must be developed to assist industry and local authorities in developing and protecting their systems from intrusion.

I'd like to review quickly a few key points from PDD-63.

The PDD established lead federal agencies to act as sector coordinator for each of the critical infrastructures. Lead functional agencies, DOD, Justice and FBI, CIA, and State, are also established. A senior level interagency group will coordinate federal government efforts, and a National Infrastructure Assurance Council will provide CEO level advice to the President.

As for DOT, we must work with the transportation sector to identify and establish a sector coordinator who will have the trust of each of six competing modes of transportation. We may have to look at one central location such as an educational institution or an association, or we may have to have one coordinator for each of the six modes. The sector coordinator and the sector liaison official, RADM Bert Kinghorn, must work together to assess vulnerabilities, develop a plan to reduce those vulnerabilities, develop a system to identify and prevent major attacks, and a plan to alert, contain, and rebuff and attack.

We must somehow overcome the natural reluctance of the regulatee trusting the regulator, and vice versa. We must find a way to protect information that is given to the government, not only to protect national security interests, but also the proprietary interests of the company itself.

Education and awareness is the first and perhaps the biggest challenge. How can we convince our leaders of the threat in a time of zero budget growth, either inside or out of the government. And once we make our leaders familiar with the problem, how do we convince the long term government employee or mid-level corporate manager to implement assurance policies that ultimately impact the bottom line with no immediate or obvious payback. If we take no action to invest in assuring the NAS, how will the government ever get the credibility with its own industries.

To protect our critical infrastructures, both government and industry alike must stop thinking solely in terms of terrorism. While we scramble to protect our planes and ships against bombs, we do little or nothing to protect the information systems that could not only compromise safety, but the nation's economic security as well as the competitiveness and perhaps the future of individual corporations.

I'd like to highlight an excellent example of a grass roots effort to improve the security of information infrastructure. In Seattle, an information security manager for a large medical group realized he did not have the tools necessary to do his job. Working with other security managers within the area, including federal, state and local governments and many other corporations, a loose knit organization called the Agora arose. Using largely a virtual network, this group of information security professionals established an extremely effective information sharing network whose sole purpose is to raise the lever of information security among those 100+ members. Once we all recognize the value to our critical systems and business processes, this type of grass roots efforts could form the basis for a national information sharing process that will evolve into a trusted network of security professionals working together to strengthen our nation and its economy. Building on these grass roots efforts, individual agencies can then provide support in areas of threat briefs and warnings, training and awareness programs. Government must be a partner in those efforts.

But we must also be careful. Government must be sure it can protect sensitive corporate information that would normally be releasable under the Freedom of Information Act, or state sunshine laws. Government must also put its own house in order, by securing critical systems such as the National Airspace System and its own information infrastructure.

From the private side, how can the federal government facilitate protection of information systems that are closely linked and critical to the nation, such as the railroad computer systems. Considering their nature, sharing data for operating the nation's rail system, while providing on-line customer service for shippers to locate their product, how do we test and strengthen these systems from penetration. And ultimately what is the government's role. The government can start by inviting play by the private sector and other agencies in DOD infrastructure based exercises.

That concludes my remarks. I'd love to hear any ideas you may have in solving some of these issues, particularly that of the government-private sector coordinator.

Joint Logistics Technology Office

Transportation Security and The Information Infrastructure

Briefing to

14th Annual NDIA Security Technology Symposium

Mr. J. Brian Sharkey
Director
(703) 696-2353
bsharkey@darpa.mil

DARPA Mission

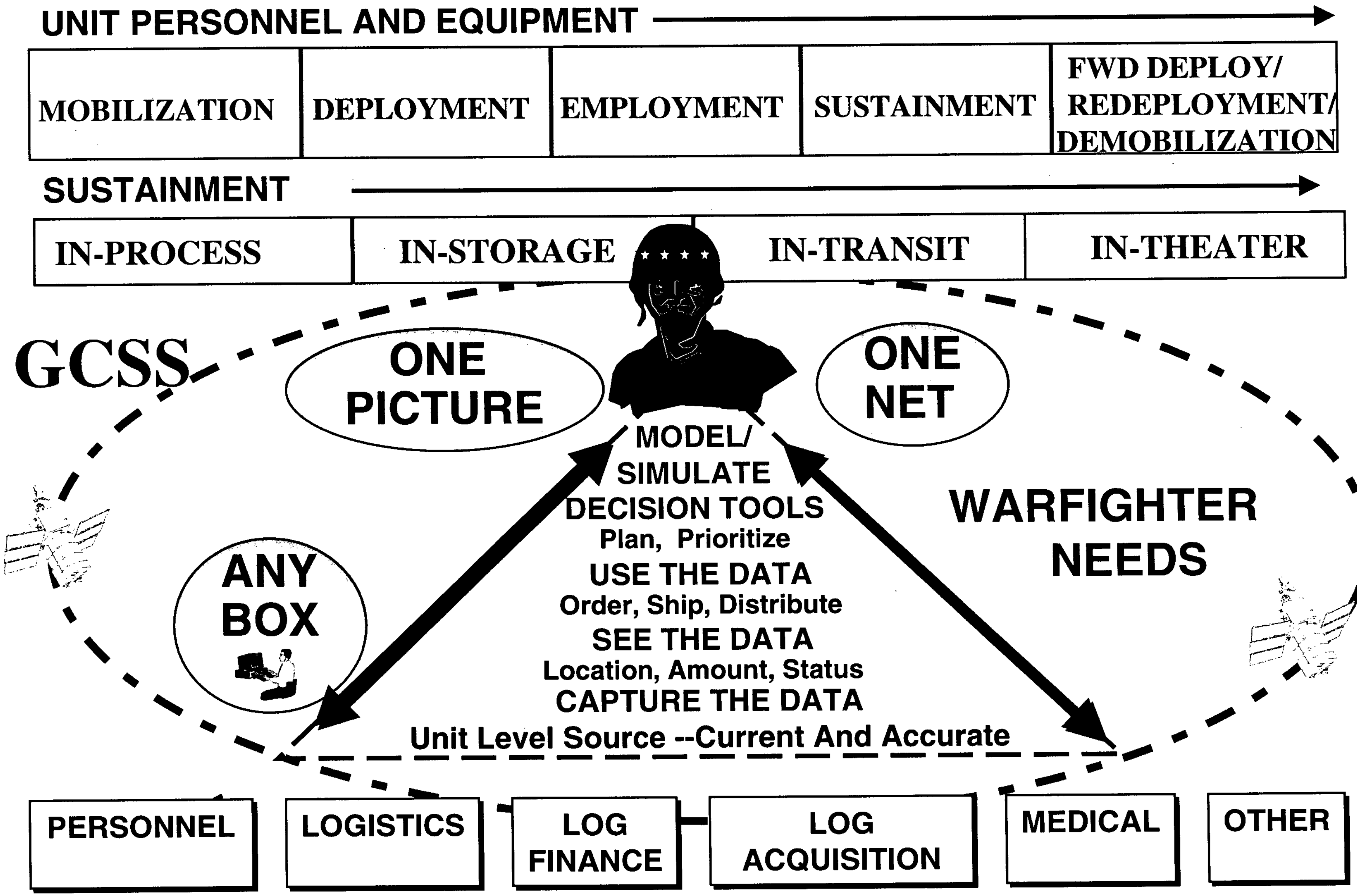
- Central R&D Organization of the Department of Defense
  - —Maintain Technology Superiority
- Pursue Imaginative & Innovative R&D Projects
- Direct R&D Projects
  - —Basic Research
  - —Applied Development
  - —Feasibility Demonstration for Improved Cost & Performance of Systems
- Cause Fundamental Change in Technology, Industrial Capability & Military Capability

Transportation and The Information Infrastructure

- The Great Reversal*
  - Communicating Information Relied on Transportation
  - Transportation Relies on Communicating Information
- Transportation System Security
  - Highly Visible Terrorist Targets
  - Increasingly Vulnerable to Cyber Attack
    - Not Physical
    - Remotely and Anonymously Affected
    - Cumulative Effect Not Easily Detected
    - Trend Towards Open Systems/Web Architecture Permits:
      - Wide Interchange Among Systems
      - Increasing Reliance on Other Systems and Data Leads to Potential for Widespread Failure
      - Introduces Greater Variety and Number of Penetration Points

* The Great Reversal: Information and Transportation Infrastructure in the Intermodal Vision, Rainer Alt, Paul W. Forster, and John Leslie King, Transportation Research Board National Conference on Developing a Research Framework for Intermodal Transportation, 1996

Global Combat Support System



UNIT PERSONNEL AND EQUIPMENT

MOBILIZATION | DEPLOYMENT | EMPLOYMENT | SUSTAINMENT | FWD DEPLOY/ REDEPLOYMENT/ DEMOBILIZATION

SUSTAINMENT

IN-PROCESS | IN-STORAGE | IN-TRANSIT | IN-THEATER

GCSS

ONE PICTURE

ONE NET

ANY BOX

MODEL/ SIMULATE DECISION TOOLS
Plan, Prioritize

USE THE DATA
Order, Ship, Distribute

SEE THE DATA
Location, Amount, Status

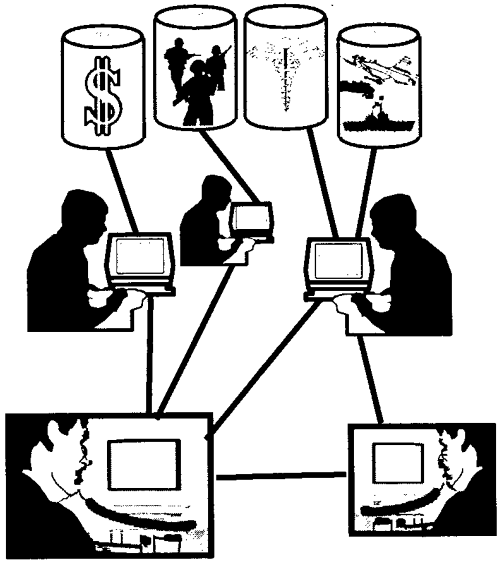
CAPTURE THE DATA
Unit Level Source --Current And Accurate

WARFIGHTER NEEDS

PERSONNEL | LOGISTICS | LOG FINANCE | LOG ACQUISITION | MEDICAL | OTHER

Global Combat Support System

DARPA



TODAY
- Many Nets
- Many Boxes
- Selected Users
- Many Pictures

TOMORROW
- One Net
- Any Box
- Any User
- Many Pictures

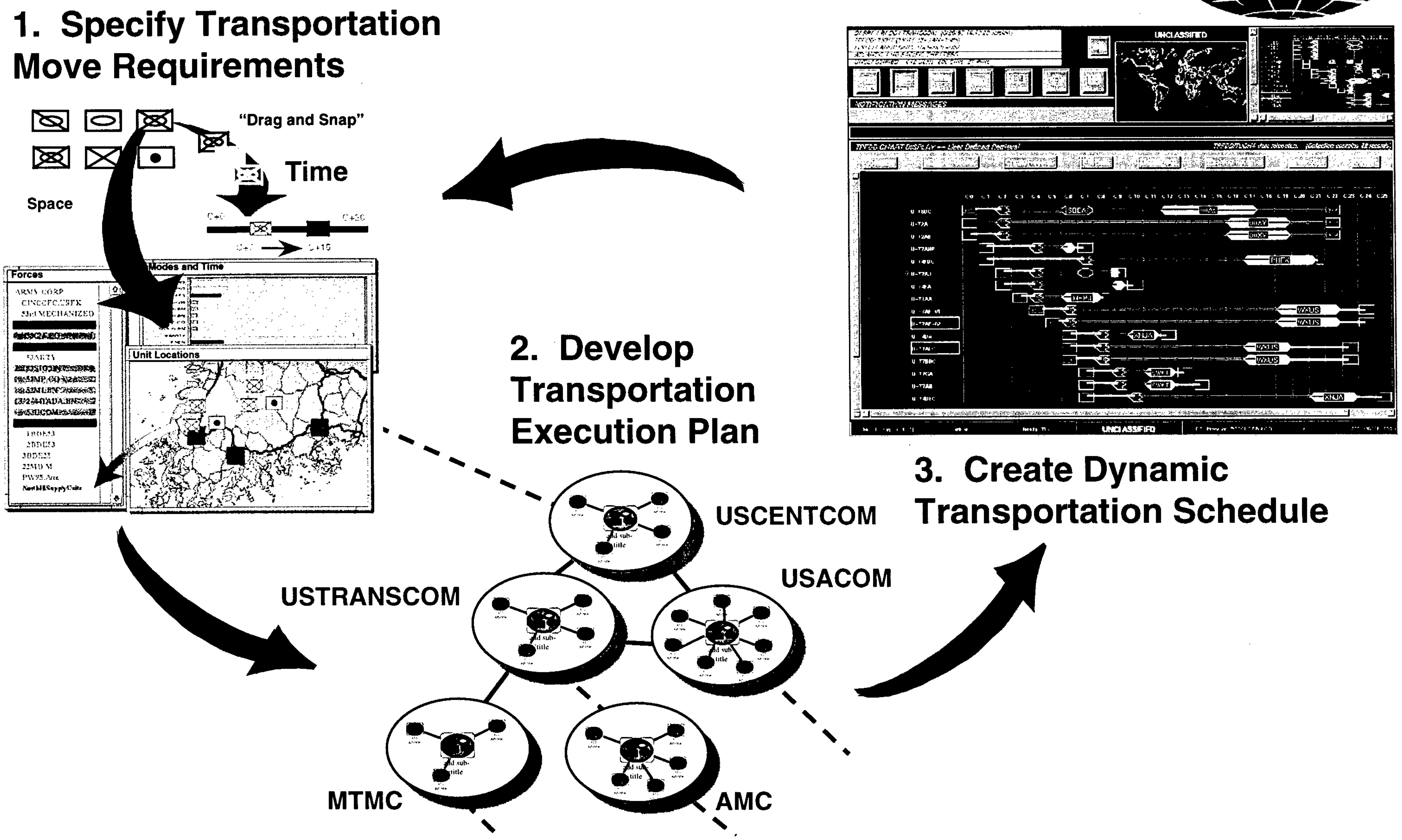
GCSS
Info
Send
Search Area
GCSS

Type: Garrison
Quantity: 2
GPS: 20' 35"
Notes:

Destination:
Combat area/
ETA: 0600

FUTURE
- One Net
- Any Box
- Any User
- One Picture

Advanced Logistics Program

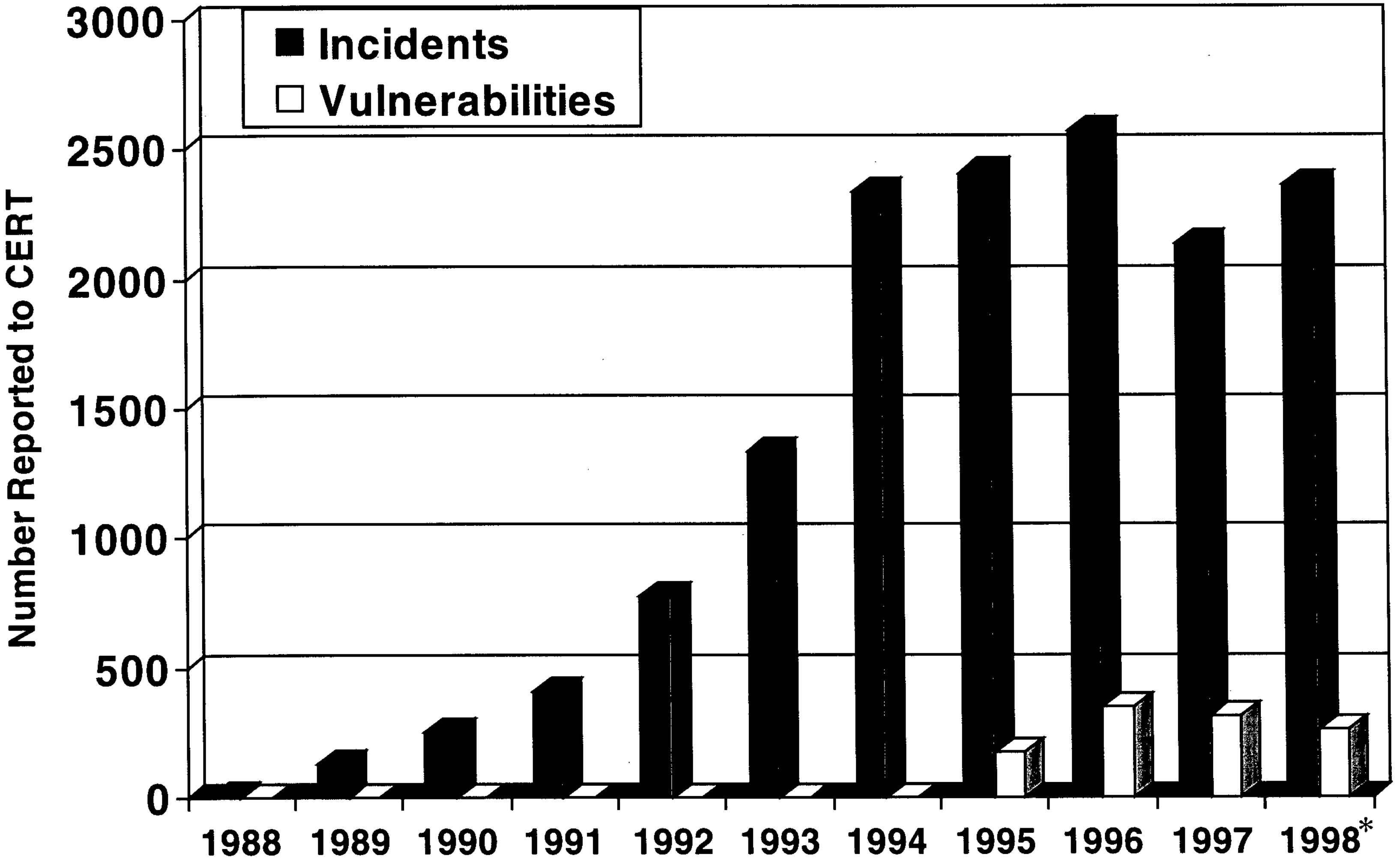


1. Specify Transportation Move Requirements

2. Develop Transportation Execution Plan

3. Create Dynamic Transportation Schedule

Trends in Attacks on Computer Systems

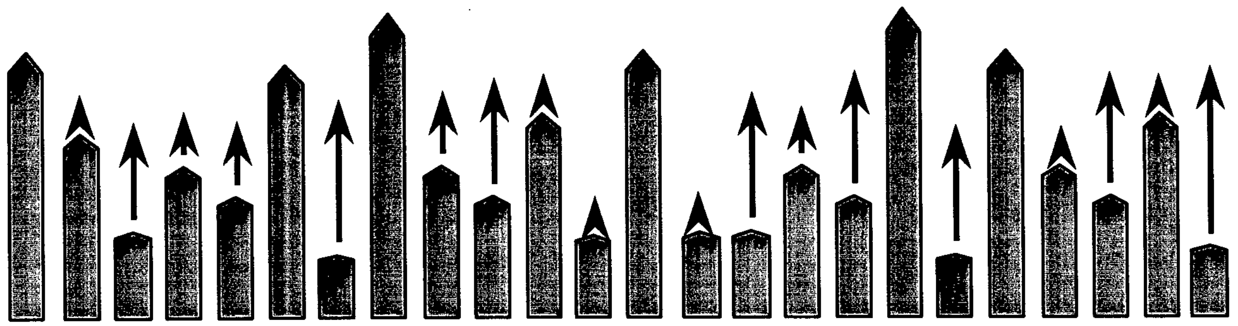


* Projected from 1st Quarter

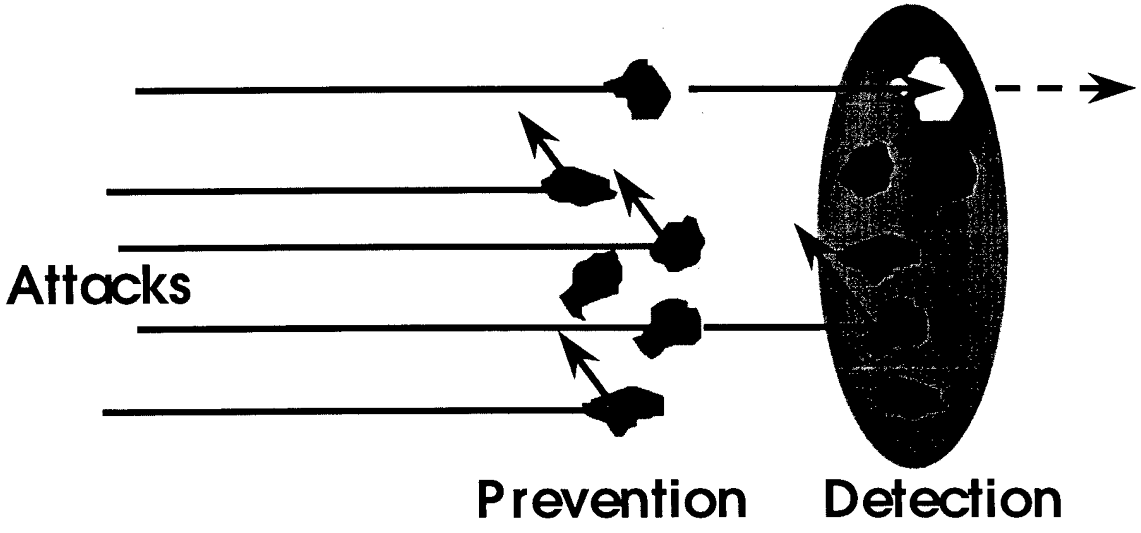
Source: CERT Coordination Center: http://www.cert.org/stats/cert_stats.html

Information Assurance Approach

- Seek a Risk-Balanced Strategy



- Prevent What You Can, Detect Residue



- Risk reduction is the name of the game
- Need tools and techniques to map vulnerability landscape
- Need model of adversary behavior
- Take game theory view
  - Min-max chess problem

Approach Supports Increased R&D Investment Strategy of PCCIP Implementation Strategy Objective 7: “Usable Tools to Fill Gaps in Technology”

Summary

- Transportation Efficiency Improvements Increasingly Dependent Upon Information Technology
  - Open Access to Data Bases and Distributed Information Processing Technologies
  - Networks (Internet, etc.)
- Potential Information Systems Solutions
  - Web Based and Other Distributed System Technologies
  - Next Generation Distributed Agent Based Architectures
- Therefore, Transportation Infrastructure Risks Need to Include Information Infrastructure Security Risks
- Information Assurance Strategies Urgently Needed
  - Risk-Balanced
  - Combined Prevention and Detection

Current and Future Trends in Cargo Security

Ed Badolato, Chairman NCSC

14th Annual Security Technology Symposium

Williamsburg, VA June 17, 1998

A Snapshot of Cargo Crime Today

-Annual US loss of $10 billion

-300,000 mid level jobs lost

-High consumer cost

-$30 billion lost worldwide

-The "Bermuda Triangle"

Rapid Change in the Cargo Industry

-Unprecedented growth
-Land Bridge America
-Upgrading the infrastructure
-Speed in handling cargo
-Automation of system

Today’s Cargo Crime

-New breed of cargo crook

-Cargo as a common denominator

-Rise of international crime

-Reluctance to prosecute cargo crime

-Rapid changes in the cargo industry

Emerging Illegal Cargo-related Activities

- –Illegal distribution of trade mark goods
- –Illicit arms, drugs, and aliens
- –Trafficking in human body parts
- –Shipment of smuggled nuclear, biological, and chemical material
- –Trafficking in endangered species

The Cargo Crook of the 90's

–Smarter, adaptive, better equipped

–Understands transportation industry

–Uses drug trafficking knowledge

–Insider connection

–Seeks high payoffs with low chance of apprehension

Objectives of Criminals Involved in Cargo Theft

- High Profits
- Avoid arrest & prosecution

Cargo Crook Categories

- Insiders
- Crews
- Organized Crime

Insiders

- 80% of cargo theft involves insiders
- Weakens cargo security initiatives
- Identifies most desirable high value goods
- Can actively participate or remain passive

Entrepreneurial Crews Operating in the US

-Central & South American

-Mexican

-West African

-Russian

-Eastern European

-Asian

Organized Crime's Common Denominators

-Drugs
-Money laundering
-Terrorism
-Smuggling
-Diversion

How Criminals Coordinate Cargo Theft

- Locate High Value Shipments--*Insiders*
- Seize Control--*Crew*s
- Remove and take to drop site--*Crews*
- Profitably Dispose of Cargo--*Fences*
- Split profits--*Mob*

Latest Organized Crime Cargo Trends

-Rapid shift to pursue new activities

-Diversifying into commercial and information enterprises

-Using sophisticated management and entrepreneurial techniques

Common Cargo Theft Methods

–Insider collusion

–Fraudulent documentation

–Covert/armed theft from trucks and warehouses

"The theft of cargo has become so widespread that it constitutes a serious threat to the flow of commerce in the United States."

(FBI Report: 1996)

Technical Precautions for Truck Cargo Security

- Install Anti-hijack Equipment
- Locked/Alarm Cab Doors
- Rooftop Marking for vehicles
- Protective Glass
- Electronic Tracking
- Coordinate Shipping with Local Police Agencies

Cargo Facility Physical Security

- Fencing
- Lighting
- Entrances
- Locks
- Alarm and Intrusion Detection Systems
- Access Controls
- Communications
- Security Guards

12 Ways To Cut Cargo Theft

- Control facility entrances and exits
- Monitor cargo and personnel movements
- Move POV parking areas away from cargo
- Screen new employees
- Investigate all cargo losses
- Establish a key control system
- Provide an adequate security force
- Install intrusion detection and access control devices
- Maintain adequate lighting and fencing
- Store all cargo in controlled security areas
- Develop close liaison with law enforcement
- Ensure continual management supervision and presence

A National Strategy for What Needs to Be Done

–Benchmark industry best practices

–Support Multi-jurisdictional Cargo Theft Task Forces

–Develop theft information and data

–Correct chronic underfunding of law enforcement activities

–Increase legal penalties

–Focus R&D efforts on the problem

Four Key Cargo Security R&D Areas

-Tracking

-Containers, Seals and Locks

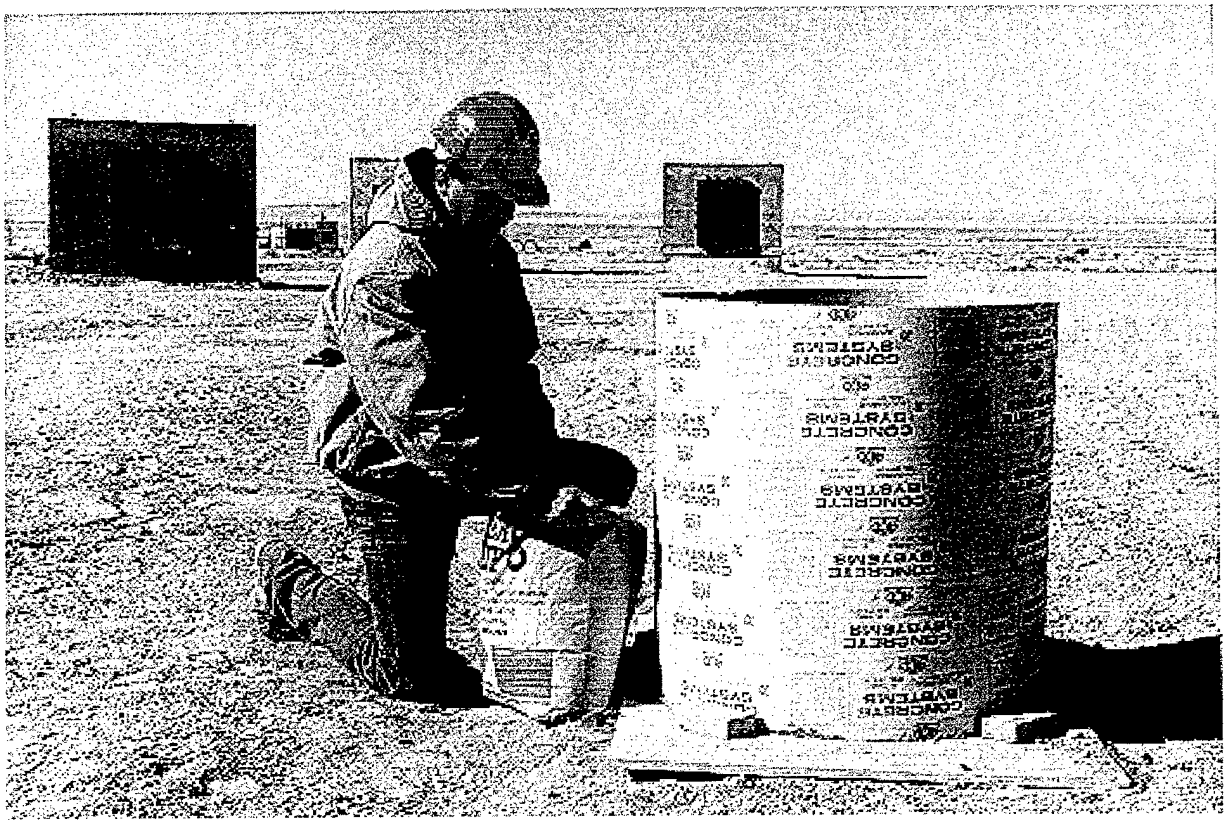
-Non-Intrusive Detection

-Physical Security & System Integration

Cargo Crime Trends

- Insiders/Crews
- Mob infiltration
- Increased fraud
- Widening intelligence information gap
- Stealing to order
- Transportation & distribution centers

Mitigation of Glass Fragment Hazards In Terrorist Bombings



Presented at the 14th Annual NDIA Security Technology Symposium & Exhibition Session VIII A: Physical Security Technologies

June 17, 1998

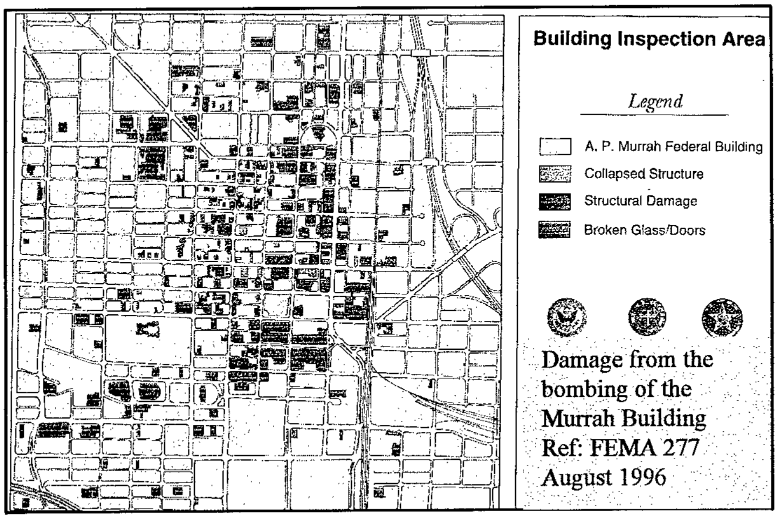
Speaker: **Mr. Joseph L. Smith**

Director of Security Engineering
Applied Research Associates, Inc.
112 Monument Place
Vicksburg, MS 39180
jsmith@ara.com **601-638-5401 ph**
601-634-4713 fax

Co-Authors:	**Mr. Bruce Hall**	**U.S. General Services Administration**
	Mr. Mark O. Oakes	**Intellimar, Inc.**
	Mrs. Nancy Renfroe	**Applied Research Associates, Inc.**

Mitigation of Glass Fragment Hazards In Terrorist Bombings

Propelled by the forces of a terrorist bomb, glass fragments may cause large numbers of serious injuries. While heavy structural damage and collapse is generally local in nature, even for a large bomb like that used in Oklahoma City, hazardous glass fragments may pose significant hazards to people in areas far removed from the attack. This is illustrated in the damage survey at the right.



Damage from the bombing of the Murrah Building Ref: FEMA 277 August 1996

Window systems consist of the glass pane, gaskets and sealants, the window frame and the anchorage to the supporting wall surface. In order to achieve a given measure of blast resistance, it is imperative that the entire window system be designed to balance the relative capacities of the system components. For example, it makes little sense and may actually introduce additional hazard to design a window system in which the glazing is stronger than the supporting frame or its attachment to the building. In such a case, the glazing may pop out and the entire assembly may be thrown into occupied spaces. A balanced design is required.

The blast capacity of glass, that is the pressure and impulse necessary to cause the glass to fail, is controlled by the type and thickness of the glass and the size of the window opening. Assuming that a window system design is balanced, thicker glass panes will provide higher blast capacities. Likewise, blast capacity is increased as the size of the window opening decreases. Glass material type will also influence capacity. Thermally tempered glass (TTG), for example, has a breaking strength that is approximately twice that of heat strengthened glass (HSG) and nearly four times that of annealed glass (AG). Glass type also influences potential hazards of the glass fragments and shards after glass failure. TTG, for example, will fail in smaller clumps or cube shaped fragments that generally pose a lower hazard than the dagger like shards produced from failing annealed glass. Hence, one effective approach to reducing the potential hazards from window glass is to design fewer and smaller windows with thicker and stronger glass that fails with lower hazard fragment sizes and shapes.

Blast resistant window technology and design procedures are readily available. Such windows have been designed and built for the military, the State Department, and other Government agencies as well as commercial/industrial users for many years. Truly blast resistant windows that are designed to fully resist a blast event provide the highest level of security and safety. However, they tend to be limited in size, expensive and are not always aesthetically pleasing. Hence, while available, fully blast resistant windows may not be practical when the goal is to provide a measure of protection to many hundreds of public buildings. As members of a free and open democratic society we expect and demand that our approach to security not be oppressive or reflect a bunker-like mentality.

With the heightened concern about terrorism in this country and the perceived need to protect not only limited high value target facilities but many facilities, an urgent need was created to develop practical and affordable techniques to limit or mitigate the potential hazards from flying glass fragments and shards. In response to this need, the US Government and private industry are developing and testing new technologies to mitigate hazards to people in the vicinity of a terrorist bombing. In cooperation with the US Army Corps of Engineers (USACE), Defense Special Weapons Agency (DSWA), US General Services Administration (GSA) and several private companies, Applied Research Associates (ARA) conducted several tests to assess the capability of methods to reduce the hazards of flying glass shards after failure of the window system. Controlling post-failure behavior does not provide as great a level of protection as designing the windows to fully resist the blast forces, but this approach does provide a practical and prudent means of reducing potential risks.

Tests were conducted in 1996 through 1998 using C4 (a military plastic explosive) and ANFO (an easy to make improvised explosive). Mounted in enclosed concrete reaction structures, the window systems evaluated included annealed, heat treated, and thermally tempered glass encompassing a wide range of monolithic, laminated and insulated configurations. Both non-responding steel frames as well as commercially available aluminum frames were evaluated. High and normal speed photography in conjunction with active pressure measurements were used to document window responses. Control specimens with no protection were also included in the tests to demonstrate the potential hazards of uncontrolled glass failure. Other samples were retrofitted with single extrusion and multi-layer security window films of 4, 6, 7 and 11 mil thickness. Laminated glass was evaluated in deep rebated frames. Finally, blast curtains that are commonly used in the U.K. to catch glass fragments after failure were also evaluated. The tests included in this paper are described in Tables 1 and 2.

All tests were performed using the GSA's "Standard Test Method for Glazing and Glazing Systems Subject to Airblast Loadings." This test method was adapted from the methods presented in the ASTM method F1642-96. All windows tested were nominally 48 by 66 inches (pane dimensions) with a 46 by 64 inch clear opening. Witness panels were located 110 and 116 inches behind the windows in test series 1-3 and 4-7, respectively. These foam panels were used to record glass fragment impacts.

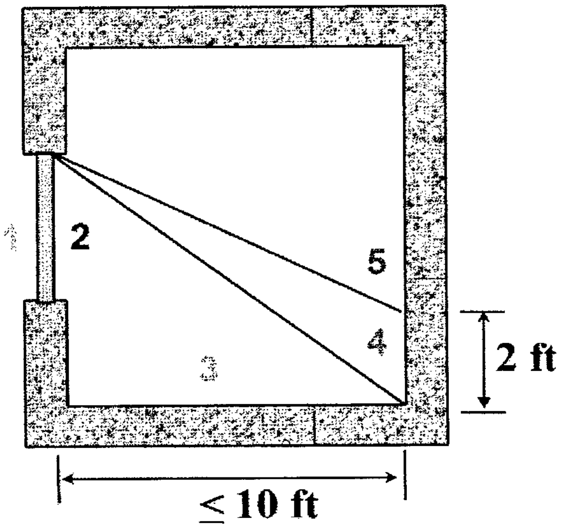
Table 1: Test location and blast description.

Test Series Location	Sponsor Test Conductor	Date	Explosive Charge
1. Fort Polk, LA	GSA USACE	July 8 – 18, 1996	420-lb, C4 (500 – lb TNT equivalent)
2. Fort Polk, LA	GlassLock USACE / ARA	August 12-22, 1996	420-lb, C4 (500 – lb TNT equivalent)
3. Fort Polk, LA	Monsanto USACE	August 29-30, 1996	420-lb, C4 (500 – lb TNT equivalent)
4. Kirtland AFB, NM	3M DSWA / ARA	January 12-19, 1998	600-lb, ANFO (500 – lb TNT equivalent)
5. Kirtland AFB, NM	GlassLock DSWA / ARA	January 22, 1998	600-lb, ANFO (500 – lb TNT equivalent)
6. Kirtland AFB, NM	Skyline Mills / Intellimar DSWA / ARA	January 26, 1998	600-lb, ANFO (500 – lb TNT equivalent)
7. Kirtland AFB, NM	GlassLock DSWA / ARA	March 5, 1998	600-lb, ANFO (500 – lb TNT equivalent)

Table 2: Description of windows tested.

Test Series Location	Number of Windows	Type of Windows	Glass thickness (in)
1	20	1. Monolithic TTG 2. Laminated TTG	1. ¼, 3/8, ½ 2. 1/8+1/8, 3/16+3/16, ¼+¼
2	20	1. Annealed (AG) 2. Thermally Tempered (TTG)	1. ¼, 3/8 2. ¼, 3/8, ½
3	8	1. Laminated AG 2. Monolithic AG 3. Laminated Heat Strengthened (HSG)	1. 1/8 + 1/8, insulated^1 2. ¼, insulated^1 3. 1/8+1/8, ¼+¼
4	24	1. Monolithic AG 2. Monolithic TTG 3. Monolithic Heat Strengthened (HSG)	1. ¼ 2. ¼, 3/8, ½, insulated^2 3. ¼
5	4	1. Monolithic TTG 2. Monolithic HSG	1. ¼ 2. insulated^2
6	4	1. Monolithic AG 2. Monolithic TTG	1. ¼ 2. ¼
7	4	1. Monolithic TTG 2. Monolithic AG	1. ¼ 2. ¼
Note: Insulated glass consists of: insulated^1 = ¼ - inch glass + ¼ - inch airspace + ¼ - inch glass insulated^2 = ¼ - inch glass + ½ - inch airspace + ¼ - inch glass			

The GSA's glazing performance standard was used to evaluate the performance of the window specimens. This standard rates the potential hazards and protection level of window systems based on the post-event location of the glass fragments and shards. Fragments that enter occupied spaces at high velocity will travel further into the space and pose a higher level of hazard to occupants. Hence, the GSA performance standard indirectly rates the hazard of fragments based on the velocity of the fragments entering protected spaces. This standard is illustrated at the right.



GSA's method of evaluating the protection offered by various window configurations is similar to the rating schemes used by the British. The only significant differences are that the British scheme places condition 3 at a distance of one meter (3.3 ft) from the window and condition 4 at a distance of one-half meter above the floor. The five conditions shown indicate the location of fragments and/or shards after failure. The conditions are defined as follows:

Table 3: GSA protection levels (Ref: GSA Security Criteria – January 17, 1997).

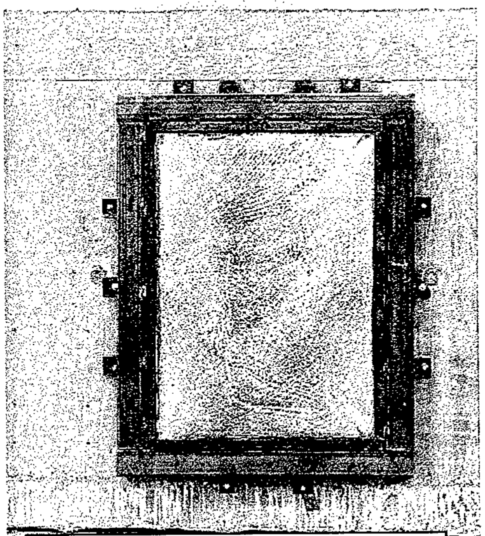
Condition	Protection - Hazard Level	Description
1	Very High Protection – No Hazard	Glass does not break.
2	Very High Protection – Very Low Hazard	Glass cracks but is retained by the frame.
3	High Protection – Low Hazard	Glass fails. Fragments enter space but land on floor no further than 10 ft from the window.
4	Medium Protection – Medium Hazard	Glass fails. Fragments enter space but land on floor or impact witness panel at a distance of 10 ft at a height no greater than 2 ft above the floor.
5	Low Protection – High Hazard	Glass fails catastrophically. Impacts on witness panel at a distance of 10 ft at a height more than 2 ft above the floor.

Twenty-one tests were performed and are reported in this paper. These tests included a total of 84 window test specimens. The results of the tests are briefly summarized in Table 4. The table presents a brief description of the test article, the window response in terms of the GSA protection condition in accordance with Table 3, and the pressure and impulse recorded during the test. Peak pressures ranged from 3.5 to 11.5 psi and impulses ranged from 23.9 to 50.5 psi-msec. Specimen responses ranged from 1 to 5 on the GSA scale. Details of the test results are available in the individual test series data analysis and test reports.

The hazard mitigation techniques evaluated showed significant potential for reducing the hazards from glass fragments. As expected, thermally tempered glass failed in a less hazardous manner than annealed or heat strengthened glass. Laminated glass and glass protected with mechanically attached film provided similar levels of protection under the tested conditions.

In general, the following are some major observations from the tests:

- Laminated glass can be engineered to withstand significant blast loads provided that adequate framing is provided. The failure mode for the laminated glass samples tended to be pull-out of the glass pane from the window bite.



Test Series 7 Window 1 Post Test: This ¼ inch thick TTG window was protected with a 7 mil thick film attached on four sides to the window frame. The glass broke but was retained by the film and the frame.

- Properly installed security window film provided significant hazard mitigation. Film generally performed better when applied to thermally tempered as opposed to annealed glass. The annealed glass at higher pressure levels initiated tears in the film which lowered the overall protection performance. Increasing film thickness generally improved the performance of the films evaluated. In addition, mechanically attached film provided better protection than daylight installed film especially at pressure levels above about 4 psi. In general, there was little observable difference in the performance of edge to edge film and daylight installed film for the limited number of samples examined. Finally, wet glazed film installations where the film is adhered to the window frame with a structural sealant appeared to provide high levels of protection.

- The blast curtain evaluated provided protection up to the tested 4 psi peak overpressure. The test results, shown on the last page of this paper (test series 6 window 3), achieved a GSA protection level 3. With additional engineering, the blast curtain technology may be capable of providing similar protection at higher blast environments. In addition, this technology may be used in conjunction with laminated glass and/or filmed glazing.

Table 4: Results of explosive tests on various window systems.

Test Series Location	**Test No.**	**Window 1** Description GSA Condition	**Window 2** Description GSA Condition	**Window 3** Description GSA Condition	**Window 4** Description GSA Condition	**Nominal Peak Pressure (psi)/Impulse (psi-msec)**	**Stand off (ft)**
1	1	¼" mono TTG, no PCM	1/8" + 1/8" Laminated TTG, no PCM	¼" mono TTG, 7 mil EE	¼" mono TTG, 7 mil 4-sided attachment	4.0/26.9	223
		3	**2**	**3**	**2**		
	2	3/8" mono TTG, no PCM	3/16" + 3/16" Laminated TTG, no PCM	3/8" mono TTG, 7 mil EE	3/8" mono TTG, 7 mil 4-sided attachment	6.0/38.9	170
		3	**3**	**3**	**2**		
	3	½ " mono TTG, no PCM	¼" + ¼" Laminated TTG, no PCM	½" mono TTG, 7 mil EE	½" mono TTG, 7 mil 4-sided attachment	8.0/42.8	142
		3	**1**	**3**	**3**		
	4	¼" mono TTG, 7 mil EE	¼" mono TTG, 7 mil 4-sided attachment	1/8+1/8 Laminated TTG, no PCM	¼" mono TTG, 7 mil 4-sided attachment	5.0/33.6	191
		3	**3**	**2**	**3**		
	5	½" mono TTG, 7 mil EE	½" mono TTG, 7 mil 4-sided attachment	¼" + ¼" Laminated TTG, no PCM	½" mono TTG, 7 mil 4-sided attachment	10.0/52.0	125
		3	**2**	**3**	**3**		
2	1	¼" mono TTG, no PCM	¼" mono TTG, 7 mil 4-sided attachment	¼" mono AG, no PCM	¼" mono AG, 7 mil 4-sided attachment	3.5/23.9	247
		5	**2**	**5**	**2**		
	2	3/8" mono TTG, no PCM	3/8" mono TTG, 7 mil 4-sided attachment	½" mono TTG, no PCM	½" mono TTG, 7 mil 4-sided attachment	6.0/35.5	170
		3	**1**	**1**	**1**		

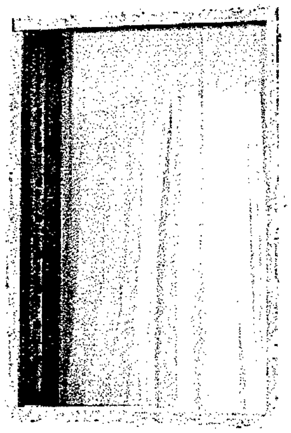
Test Series Location	Test No.	Window 1 Description GSA Condition	Window 2 Description GSA Condition	Window 3 Description GSA Condition	Window 4 Description GSA Condition	Nominal Peak Pressure (psi)/Impulse (psi-msec)	Stand off (ft)
2 (con't)	3	3/8″ mono AG, no PCM	3/8″ mono AG, 7 mil 4-sided attachment	3/8″ mono TTG, no PCM	3/8″ mono TTG, 7 mil 4-sided attachment	7.0/43.0	150
		5	**3**	**5**	**2**		
	4	¼″ mono AG, 7 mil day-light PCM	¼″ mono AG, 7 mil 4-sided attachment	¼″ mono TTG, 7 mil day-light PCM	¼″ mono TTG, 7 mil 4-sided attachment	5.0/30.8	191
		3	**3**	**2**	**2**		
	5	¼″ mono TTG, 7 mil 4-sided attachment	¼″ mono AG, 7 mil 4-sided attachment	¼″ mono TTG, 7 mil 2 vertical edges attached	¼″ mono TTG, 7 mil top edge attached	4.0/27.8	223
		2	**3**	**2**	**2**		
3	1	¼″ laminated AG, no PCM	¼″ laminated HSG, no PCM	¼″ mono AG + ¼″ air + ¼″ laminated AG	¼″ mono AG, no PCM	4.0/27.7	223
		2	**2**	**2**	**5**		
	2	½″ laminated AG, no PCM	½″ laminated HSG, no PCM	¼″ mono AG + ¼″ air + ¼″ laminated AG	¼″ laminated AG + ¼″ air + ¼″ laminated AG	8.0/48.9	133
		3	**3**	**3**	**2**		
4	1	¼″ mono AG, *4 mil day-light PCM	¼″ mono AG, *4 mil 4-sided attachment	¼″ mono AG, 7 mil 4-sided attachment	¼″ mono AG, no PCM	4.2/28.4	190
		3-SHR	**3-SHR**	**3-SHR**	**5**		
	2	¼″ mono HSG, *4 mil 4-sided attachment	¼″ mono TTG, *4 mil 4-sided attachment, aluminum frame	¼″ mono AG, *4 mil 4-sided attachment, aluminum frame	¼″ mono AG, *4 mil 2-sided vertical attachment	4.1/28.7	190
		3-SHR	**3-SHR**	**5-SHR**	**3-SHR**		
	3	¼″ mono TTG, *4 mil , 4-sided attachment	¼″ mono TTG, *6 mil , 4-sided attachment	¼″ mono HSG, *6 mil , 4-sided attachment	¼″ mono TTG, *4 mil , daylight	5.3/33.4	165
		3-SHR	**2**	**3-SHR**	**3**		
	4	¼″ mono AG, *6 mil , 4-sided attachment	¼″ mono TTG, *4 mil 4-sided wet glaze, aluminum frame	¼″ mono AG, *4 mil 4-sided wet glaze, aluminum frame	¼″ mono TTG, *4 mil 4-sided attachment	4.1/29.0	190
		3	**2**	**3-SHR**	**3-SHR**		
	5	3/8″ mono TTG, *4 mil, 4-sided attachment	½″ mono TTG, *6 mil, 4-sided attachment	½″ mono TTG, *4 mil, 4-sided attachment	3/8″ mono TTG, *4 mil, day-light	9.1/49.6	121
		3	**2**	**5-SHR**	**3-SHR**		
	6	¼″ mono TTG, *4 mil, daylight	¼″ mono TTG + ½″ air + ¼″ mono TTG, *4 mil, 4-sided attachment	¼″ mono TTG + ½″ air + ¼″ mono TTG, *6 mil, 4-sided attachment	¼″ mono TTG + ½″ air + ¼″ mono TTG, no PCM	9.0/49.6	121
		5	**3-SHR**	**2**	**5**		

Test Series Location	Test No.	Window 1 Description GSA Condition	Window 2 Description GSA Condition	Window 3 Description GSA Condition	Window 4 Description GSA Condition	Nominal Peak Pressure (psi)/Impulse (psi-msec)	Stand off (ft)
5	1	¼" mono TTG, 11 mil, 1-sided attachment	¼" mono HSG + ½" air + ¼" mono HSG, 7 mil, 2 sided vertical attachment, aluminum frame	¼" mono HSG + ½" air + ¼" mono HSG, 11 mil, 2 sided vertical attachment, aluminum frame	¼" mono HSG + ½" air + ¼" mono HSG, no PCM	8.7/48.2	124
		3-SHR	**5**	**5-SHR**	**5**		
6	1	¼" mono AG, no blast curtain	Wood framed window with ¼" mono AG, 3 x 2 true division window, exterior mounted curtain	¼" mono AG, exterior mounted curtain	¼" mono TTG, interior mounted curtain	Windows 1-3 4.0/28.8 Window 4 11.5/50.5	190 110
		5	**5**	**3**	**5**		
7	1	¼" mono TTG, 7 mil 4-sided attachment	¼" mono AG, 4 mil day-light, aluminum frame	¼" mono AG, 7 mil day-light, aluminum frame	¼" mono TTG, no PCM	4.0/28.2	190
		2	**3**	**3**	**5**		

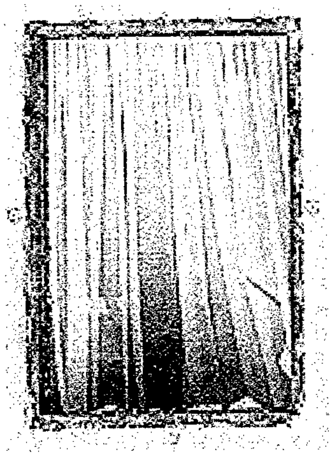
- PCM denotes Polyester Composite Material (i.e., security film). A * denotes multi-layered film.
- Film is installed in several configurations. Daylight detonates film that is applied to the visible glass surface only. EE (Edge to Edge) denotes film that is installed to the edges of the glass pane and is captured in the bite of the window frame. Attached film is installed on the glass surface and mechanically fastened to the window frame by means of a batten bar system.
- The SHR stands for significant-hazard-reduction. This designation is used to distinguish a significantly reduced glass fragment hazard obtained with a protective window system versus a highly hazardous uncontrolled failure with no protective measure that is given the same GSA hazard condition. The SHR designation can be given for GSA conditions 3-5. The SHR designation was not used in test series 1-3.
- Unless otherwise indicated, all tested window frames are steel.

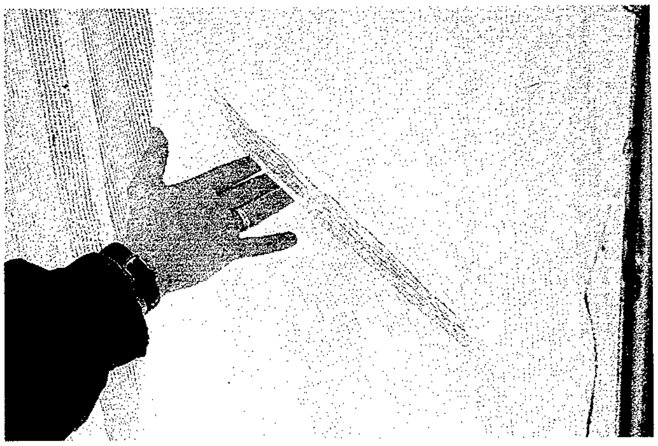
In conclusion, all of the hazard mitigation techniques (i.e., balanced window system design, appropriate selection of glass type and thickness, laminated glass, security window film and blast curtains) provided reductions in the hazards from glass fragments and shards. These methods should be employed by facility owners and occupants to reduce the potential hazards that glass failure poses to people during a terrorist bombing.

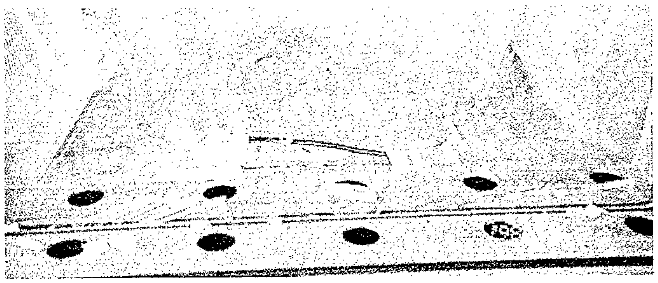
Photographs on this page illustrate performance of the blast curtain system evaluated. (Test series 6, window 3)



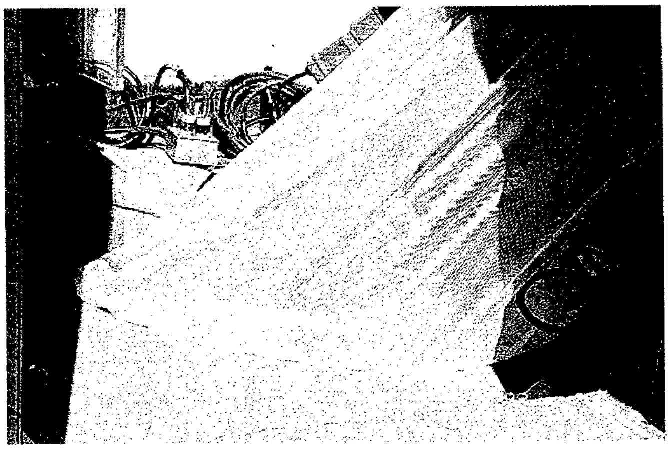
Pre- and Post-test exterior views of the window protected with Skyline Mills blast curtain system.







Looking into the reaction structure from the outside, these views show the trapped glass.



SPAWAR

Systems Center
San Diego

ADVANCED USER INTERFACE DESIGN
and
ADVANCED INTERNETTING
for
TACTICAL SECURITY SYSTEMS

Space and Naval Warfare Systems Center
San Diego, California 92152-5001

TACTICAL SECURITY ISSUES

- OPERATIONS
  - Tactical Environment
  - Joint Force Involvement
  - Diverse Missions
- TECHNOLOGY
  - Stand-alone Designs
  - Growth Provisions
  - Special Interfaces

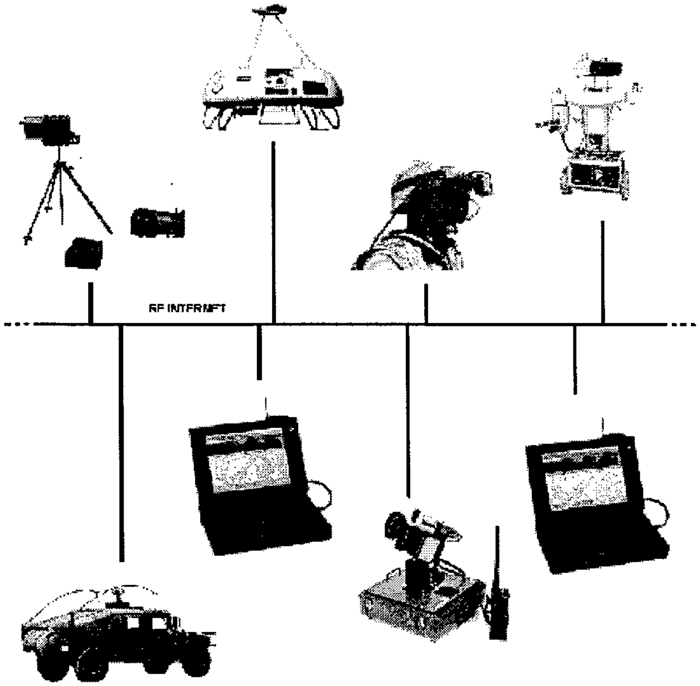
FAMILY of INTEGRATED TACTICAL SECURITY SYSTEMS

- US ARMY MP SCHOOL CONCEPT
- FORCE XX1 ARMY
- POINT and AREA SECURITY
- WAR and MOOTW
- INTEROPERABLE with JOINT FORCES
- MAN PORTABLE
- OPEN ARCHITECTURE
- MAXIMUM USE of COTS and GOTS
- PROVIDE for TECHNOLOGICAL GROWTH

SPAWAR
Systems Center
San Diego

DSWA TECHNOLOGY PROJECTS

ADVANCED USER INTERFACE
for TACTICAL SECURITY



TACTICAL SECURITY
SENSOR INTERNETTING

AITS OBJECTIVES

- PROOF-OF-CONCEPT PROTOTYPE

  Man-portable

  Modular — “plug and play”

- TO SUPPORT

  Situation Awareness

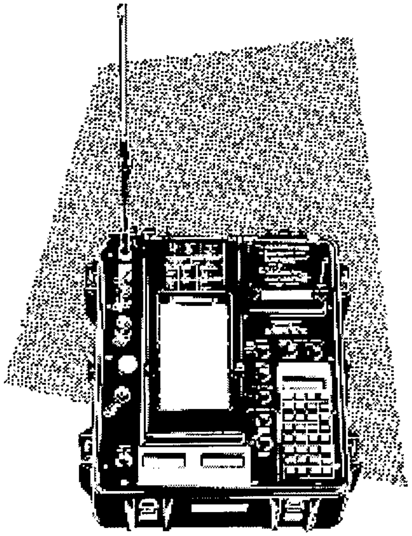
  Intuitive Operation

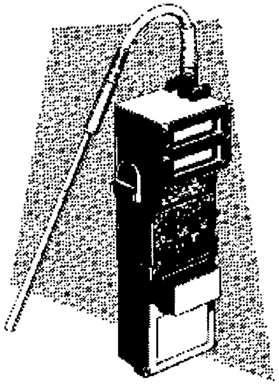
  Reduced Workload

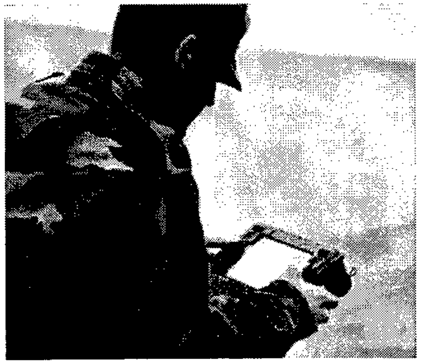
SPAWAR

Systems Center
San Diego

CURRENT INTERFACE RESOURCES







APPROACH

- PHASE 1

  Examine User Needs

  Design Interface Concept

- PHASE 2

  Build Prototype

  Validate with User Communities

  Document

INTERFACE FEATURES

- WEARABLE SYSTEM
- SEE-THROUGH DISPLAYS
- VOICE INTERACTION
- INTEGRATED COMMUNICATIONS

SPAWAR

Systems Center
San Diego

TACTICAL SENSOR INTERNETTING and INTEGRATION

- GOALS

  Effective, Robust Use of Bandwidth

  Control of Multiple Tactical Sensors

  Common Tactical Picture

  “Soldier as Sensor”

- ISSUES

  Tactical Node Handling

  Internet Overhead

  Intelligent Data Handling

SPAWAR
Systems Center
San Diego

TSSII APPROACH

- SOFTWARE PROTOCOLS ON TOP of INTERNET
- BUILD OVER UDP VICE TCP
- DIRECT ACCESS to IP FUNCTIONALITY

FOR FURTHER INFORMATION

- **ADVANCED INTERFACE**

STEVE MURRAY	STEVE MARTIN
murrays@spawar.navy.mil	martinsw@spawar.navy.mil
(619) 553-6350	(619) 553-9882

- **TACTICAL SENSOR INTERNETTING**

DALE BRYAN
bryan@spawar.navy.mil
(619) 553-1902

- **GENERAL PROJECT INFO**

http://marlin.spawar.navy.mil/D37/

COTS TEST AND EVALUATION

SESSION: Military Force Protection

AUTHOR: James A. Suarez

ADDRESS: Radian Inc.
Suite 725
5845 Richmond Highway
Alexandria, Virginia 22303-1865

TELEPHONE: (703) 329-9300 (V)
(703) 329-9510 (F)

E-MAIL: jsuarez@radianinc.com

The bombing of Khobar Towers in Dhahran, Saudi Arabia, on 25 June 1996 killed 19 American servicemen and injured hundreds more. As a result, General Wayne A. Downing (Ret.) was appointed to conduct an assessment of the bombing incident. A major finding was that technology was not widely used in order to detect, delay, mitigate, and respond to acts of terrorism. That report recommended technical assistance to rapidly acquire and quickly field integrated technology to deployed forces in the Central Command (CENTCOM) Area of Operations (AOR).

It becomes painfully obvious from the above that there is an urgent need to better protect military installations located in high threat areas from vehicle bombs and improved explosive devices (IEDs). Facilities currently use explosive detector dogs (bomb dogs) and manual searches to screen incoming vehicles. While both of these can be effective at finding suspect devices, extreme environmental conditions experienced at many installations around the world often limit the operational utility of the explosive detector dogs. In addition, manual screenings are often time consuming, labor intensive, and open to subjectivity. These facts expose a need for an improved security screening solution. Technological advances in the security technology arena have made more and better security equipment available for commercial use, but, for the most part, these technological advances have not yet been fully incorporated into the security screening process.

On the 1st of May 1997, Radian Inc. was tasked by the Physical Security Equipment Management Office (PSEMO), located at Ft. Belvoir, Virginia, to do the following:

> *Deploy COTS equipment requested by J-34 via Military Airlift Command (MAC) from Dover, AFB, enroute to the CENTCOM AOR in order to equip and train service-members assigned to Southwest Asia (SWA) in the use of an explosive particle detector; on order re-deploy via commercial air.*

It was 25 calendar days from the receipt of this requirement to the emplacement of Commercial Off The Shelf (COTS) equipment on the ground in SWA. While this quick turnaround from tasking to execution is commendable, there are issues that deserve closer analysis if we (the security industry in concert with government) are expected to be able to preserve and protect the forces abroad.

As a result of an intensive market survey, the decision to purchase a Barringer explosive particle detector had already been made prior to Radian being tasked to execute this mission. Since the users' needs revolve around a series of parameters to include the threat, application, environment, etc., the first concern is that there was absolutely no user evaluation much less operational testing conducted as part of the market survey in order to evaluate, qualify, and certify the Barringer Ionscan 400, or any other system out on the commercial market today, as ***"the solution"*** to explosive detection in SWA. This shortfall resulted in some interesting findings three to four months after fielding had been completed. The most noteworthy of these was that the sand in SWA was so extremely fine (similar to talcum powder or flour) that the filters on the back of the Barringer Detector Module (DM) and Power Pump Module (PPM) were found by the users to be unsatisfactory. Even though the manufacturer quickly responded to this problem by developing a new and improved filter, one organization at Al-Jaber, Kuwait, routinely experienced such problems with the fine sand and strong winds (> 45 mph) that they stopped utilizing their Ionscan all together and gave it up to their sister unit in Riyadh, Saudi Arabia, since they had no shelter in which to place it for operational usage. Their opinion was that the instrument would be inoperative more than operative (operationally down more than up) under those austere conditions, so they should give it to someone that was going to utilize it.

While these harsh conditions could probably never have been exactly duplicated in a laboratory environment, there were other environmental conditions that were a problem and could have been duplicated. The most memorable of these was the heat. The Ionscan operator's manual specs the Barringer 400 to be able to operate between temperature ranges of 0 degrees Celsius to 40 degrees Celsius (32 degrees Fahrenheit to approximately 104 degrees Fahrenheit). While this temperature range appears to be adequate, temperatures in SWA routinely exceeded 115 degrees in the shade! Consequently, the Ionscan had difficulty operating simply because it was not designed to operate in the extreme heat commonly found in SWA.

At this point, I would be remiss if I did not mention that the Naval Explosive Ordnance Disposal Technology Division, based out of Indian Head, Maryland, recently published an extremely comprehensive technical report which assessed how the Barringer, as well as other selected COTS items, performed in SWA during the period 13 August 97 to 11 September 97. The assessment was conducted in order to verify the limits of the Ionscan and to determine if the technology (Ion Mobility Spectrometry) could be deployed in an Entry Control Point (ECP) screening process. It was conducted in three phases. The first two phases were conducted in order to isolate and study two of the parameters effecting explosive trace detectors: detection limits and collection efficiency. The third phase of the assessment served as an opportunity to optimize protocols in preparation for the field assessment portion of the operational test.

This document is excellent and provides the reader with data which convincingly shows that despite the fact that the Ionscan has been designed for use in commercial airports and not hardened for a military application, it can be forced to work under the extremely harsh conditions found in SWA. My concern with this report is its timing. It would have been wonderful to have been able to gather some type of data ***prior to*** procurement and subsequent fielding of the Barringer instrument in order to afford the end user the best "bang for his buck" given the existing set of circumstances.

Shifting gears from the environment and the absence of any user evaluation or operational testing prior to procurement, the second point of concern focuses around the lack of a solid data collection effort. The funds provided to Radian Inc. in order to execute this task did not allow for a subsequent data collection effort of **any** type to occur after the Barringer units had been fielded. Since this raw data formulates the basis for "**lessons learned**" in the event that there should ever be a second fielding of Ionscans to SWA or elsewhere, it is absolutely critical to have some type of data base or information available should the need to purchase future Ionscans arise again. Furthermore, it should be noted that the collector of data should not ever have to be the fielded unit since that organization is already overloaded with an ongoing real world mission and as such should be allowed to focus exclusively on that duty. Instead, the burden should be placed on a support contractor or other agency. Specific information would involve but not be limited to the following: operational life of critical components, mean time between failures, difference between suggested manufacturer's maintenance schedule and what is actually required in theater due to more austere environmental conditions, etc. Additionally, the data collector and the data collection effort should be rotated from site to site wherever a piece of equipment has been deployed. In this last fielding, the only data that was collected was in the EOD technical report mentioned above. While this was certainly better than no data at all, it does not adequately address the data collection effort as a separate entity, it focuses exclusively on one site, and its publication occurred some 9 months after the fact (fielding occurred in May 97 and report was published in February 98).

The third issue of concern deals with the need for Integrated Logistical Support (ILS) and sustainment training in the theater of operations once initial fielding has occurred. Upon delivery, it becomes the responsibility of the fielded unit to take, in this case, the Barringer unit and "make it work." However, it becomes unreasonable to expect superb results if there is absolutely no in-country support in order to sustain the fielding effort. This piece was absent during the Ionscan fielding. The gaining organizations were left with appropriate publications and told that their machine had a one-year warranty with it and that they should address any problems, questions, or issues directly with the manufacturer in New Jersey. Depending on the emphasis placed by the chain of command on the success or failure of a newly acquired item, this mindset would in many cases cause an organization not to seek immediate assistance in the event difficulties operating the machine are encountered after the fielding agent or agency has departed the theater. In a scenario where the Iraqi border is 30 kilometers away and soldiers and airmen alike are working 24 hours a day, 7 days a week; calling the manufacturer in order to troubleshoot an issue simply becomes too difficult to do and not a priority of the moment. It is explicitly for that reason that there should be in the best of cases in country logistical support available. If that is not possible, perhaps support from some forward location where similar units have already been fielded should be considered.

Taking the issue of in-country support one step further, the discussion would not be complete without mentioning the issue of personnel turbulence in SWA. Since duty in SWA is considered to be a "hardship" tour, service members are assigned to SWA anywhere from 120 days to one full year. This "short tour" in theater coupled with the fact that operating the Ionscan properly is a "use or lose" skill outlines a scenario where those that are trained on the Ionscan take the knowledge with them when they rotate back to CONUS if they don't train their successors prior to departure, which is often the case. This situation clearly reinforces the need for periodic sustainment training to occur within the AOR on a recurring basis. It must be understood that the financial burden of providing in-country logistical support, sustainment training, and the data collection effort described earlier must be funded as part of the total package despite the fact that these appear to be add-on packages. While not always economical, these add-ons are extremely prudent investments. Their importance is so critical that their absence could make the difference between a successful and unsuccessful COTS fielding effort.

Finally, I would like to discuss some successes regarding Barringer's newly acquired capability of being able to support users who are located "far away" from the manufacturing facility. The first of these is Computer Based Training (CBT) which comes in the form of a CD ROM. This device is an exportable training package and, while not one-on-one instruction by a qualified Barringer trainer, offers the operator step-by-step instruction on how to do the following: set up, start up, verification/auto calibration procedures and sampling techniques using both the swab and the remote sampler. This tool will allow users to sustain their training base in areas where there is high personnel turbulence. The highlights of this package include but are not limited to the following:

1. Visualization of the traces (residue) under UV light on the hands of an individual fabricating an IED.
2. Visualization of the transfer of these traces to a doorknob and briefcase under UV light.
3. Sampling the briefcase with a swab and detecting explosive residue on the briefcase described above.
4. Convincing the operator that we can detect and isolate the invisible.

Computer Based Training is the next best thing to an instructor conducting formal academic training in a classroom environment. The 4404th Security Police Squadron (SPS) at Prince Sultan Air Base (PSAB) has purchased five of these CD ROMS and are pleased with the results.

Secondly, Barringer has recently added a capability that allows the user to query the manufacturer via the internet by having him or her enter the serial number of the machine coupled with the password for the same. This capability will afford users the flexibility to troubleshoot a problem 24 hours a day from a remote location should the need arise.

Thirdly, through hardwiring a modem to the Ionscan or using a wireless modem, Barringer has recently added the capability to collect an infinite amount of parametric data from remote locations. Information regarding the following can be tracked by Barringer: total cumulative samples and hours since the unit was fielded, daily total samples and hours, number of verifics (verifications) done per day and the time date stamp of the verific alarm, location of the calibrant peak at the time of the verific alarm, the number of alarms if any occurred and what type of compound was detected, whether or not a bakeout was done (maintenance procedure used to clean out the system) and other pertinent information can be monitored from the manufacturing facility in New Jersey. Barringer personnel can even contact users when a corrective measure is required in the field on a remotely monitored system. This is currently being done with the Federal Aviation Administration (FAA) on well over 150 of their units.

Table 1 shows an example of this capability on six different Barringer systems from which data was collected for six days (26 January to 1 February 98). Line number 7 shows 18 samples taken over a 24- hour period with zero verifics and a calibrant delta of +41, line 10 shows one alarm for PETN and lines 38, 39, and 40 show sample counts of zero yet indicate that a "bakeout" was performed on January 30th. These bits of data are "flag raisers" and are signals that perhaps deserve further explanation by the user. The units in SWA could greatly benefit from this type of support and should be tied into this network if they are expected to be successful with their Ionscan.

In summary, this particular COTS fielding effort was a tremendous learning experience for all concerned. While we recognize that there were a few shortcomings associated with this effort, we are all charged with making the process better for the subsequent COTS fieldings and challenges that lie ahead. Specific conclusions that can be made regarding the Barringer Ionscan 400 COTS fielding effort to SWA involve, but are not limited to, the following:

- User evaluations or operational testing conducted in CONUS prior to field deployment will validate the capabilities of the equipment being purchased.
- A solid data collection effort will strengthen the argument for purchasing additional devices from the same manufacturer.
- The need for Integrated Logistical Support (ILS) and sustainment training cannot be overlooked or left out of the COTS equation.
- No single technological solution exists to adequately screen vehicles or personnel for large or small explosive devices.

- Screening vehicles at entry control points impacts the routine flow of traffic. The severity of this impact is a function of thoroughness of the screening personnel. Additional personnel and control points are required to maintain throughput rates with increased security.
- The deterrence value of highly visible security equipment will exist wherever the equipment is fielded, but it cannot be measured.
- Future COTS fieldings at any operational facility must have a formal commitment by the operational Command if the fielding is expected to be a successful one.

While this paper has focused exclusively on one event, the fielding of the Barringer Ionscan to selected military installations in SWA, the ***"lessons learned"*** have a far reaching implication and can be applied to the COTS fielding activity in general.

TABLE 1

Airport Report								1998-Jan-26 to 1998-Feb-01														P
#	Date	Airport	S/N	Total Oper Time (hrs)	Total Sample Count	Daily Oper Time (hrs)	Daily Sample Count	ALARMS	DNT	NG	NIIRATE	PETN	RDX	SEMTEX	TNT	OTHER	VERIFIC	Calibrant Amplitude		Calibrant Delta		BAKEOUT
																		Max	Min	Max	Min	
1.	1998-Jan 26	ABC	9476	8926.8	105915	24.0	320	0									3	409	378	+24	+15	x
2.	1998-Jan 27	ABC	9476	8950.8	106182	24.0	267	0									3	420	342	+21	+19	x
3.	1998-Jan 28	ABC	9476	8974.8	106445	24.0	263	0									2	442	374	+15	+10	x
4.	1998-Jan 29	ABC	9476	8998.8	106716	24.0	271	0									2	448	378	+19	+11	x
5.	1998-Jan 30	ABC	9476	9022.8	106945	24.0	229	0									2	399	353	+17	+8	x
6.	1998-Jan 31	ABC	9476	9046.8	107079	24.0	134	0									1	369	315	+49	+17	x
7.	1998-Feb 01	ABC	9476	9070.8	107097	24.0	18	0									0	403	345	+93	+52	x
8.	1998-Jan 26	ABC	9485	6169.1	107138	17.1	290	0									4	530	447	+17	0	x
9.	1998-Jan 27	ABC	9485	6185.9	107497	16.9	359	0									3	503	445	+18	+1	x
10.	1998-Jan 28	ABC	9485	6203.1	107875	17.1	378	1				1					4	510	448	+16	0	x
11.	1998-Jan 29	ABC	9485	6220.1	108187	17.1	312	0									5	540	424	+9	-4	x
12.	1998-Jan 30	ABC	9485	6237.4	108548	17.2	361	0									4	553	443	-11	-5	x
13.	1998-Jan 31	ABC	9485	6254.2	108908	16.9	360	0									5	528	452	+11	-1	x
14.	1998-Feb 01	ABC	9485	6271.4	109247	17.3	339	0									3	469	410	+12	-1	x
15.	1998-Jan 26	ABC	9487	6200.8	99608	19.3	297	0									3	540	398	-11	-2	x
16.	1998-Jan 27	ABC	9487	6223.4	99942	22.6	334	0									3	474	391	-14	-4	✓
17.	1998-Jan 28	ABC	9487	6242.1	100251	18.7	309	0									3	500	455	-21	+1	x
18.	1998-Jan 29	ABC	9487	6264.6	100560	22.6	309	0									3	491	409	-29	-16	✓
19.	1998-Jan 30	ABC	9487	6281.5	100854	16.9	294	0									3	479	399	-21	-11	x
20.	1998-Jan 31	ABC	9487	6299.5	101116	18.0	262	0									3	506	402	-18	0	x
21.	1998-Feb 01	ABC	9487	6318.2	101434	18.7	318	0									3	513	398	+6	-2	x
22.	1998-Jan 26	ABC	9595	2482.5	9282	24.0	97	0									4	522	441	+7	+4	x
23.	1998-Jan 27	ABC	9595	2506.4	9350	23.9	68	0									2	508	459	+8	+1	x
24.	1998-Jan 28	ABC	9595	2530.3	9450	23.9	100	0									2	543	504	+7	+1	x
25.	1998-Jan 30	ABC	9595	2576.1	9630	47.8	180	0									2	520	452	-7	0	x
26.	1998-Jan 31	ABC	9595	2601.6	9703	23.5	73	0									3	509	456	+5	+1	x
27.	1998-Feb 01	ABC	9595	2625.5	9807	23.9	104	0									3	532	436	+9	+4	x
28.	1998-Jan 20	ABC	10074	2273.3	11623	24.0	163	0									2	504	428	+24	+21	x
29.	1998-Jan 27	ABC	10074	2297.3	11733	24.0	110	0									2	423	373	-17	+3	x
30.	1998-Jan 28	ABC	10074	2321.3	11889	24.0	158	0									2	428	382	-33	-18	x
31.	1998-Jan 29	ABC	10074	2345.3	12076	24.0	187	0									2	444	394	-49	-30	x
32.	1998-Jan 30	ABC	10074	2369.3	12210	24.0	134	0									2	464	418	-48	-41	x

Airport Report						1998-Jan-26 to 1998-Feb-01																P
#	Date	Airport	S/N	Total Oper Time (hrs)	Total Sample Count	Daily Oper Time (hrs)	Daily Sample Count	ALARMS	DNT	NG	NITRATE	PETN	RDX	SEMTEX	TNT	OTHER	VERIFIC	Calibrant Amplitude		Calibrant Delta		BAKEOUT
																		Max	Min	Max	Min	
33.	1998-Jan 31	ABC	10074	2393.2	12378	24.0	168	0									2	454	380	-38	-14	x
34.	1998-Feb 01	ABC	10074	2417.2	12506	24.0	128	0									2	453	383	-20	-7	x
35.	1998-Jan 27	ABC	10083	2681.6	10199	112.7	259	0									1	537	413	+2	+2	x
36.	1998-Jan 28	ABC	10083	2705.6	10284	24.0	85	0									3	556	512	-22	-8	x
37.	1998-Jan 29	ABC	10083	2729.6	10288	24.0	4	0									0	576	576	-28	-28	x
38.	1998-Jan 30	ABC	10083	2754.6	10288	25.1	0	0									0					✓
39.	1998-Jan 31	ABC	10083	2795.1	10288	40.5	0	0									0					x
40.	1998-Feb 01	ABC	10083	2802.6	10288	7.5	0	0									0					x
						992.9	8040	1	0	0	0	1	0	0	0	0	96					

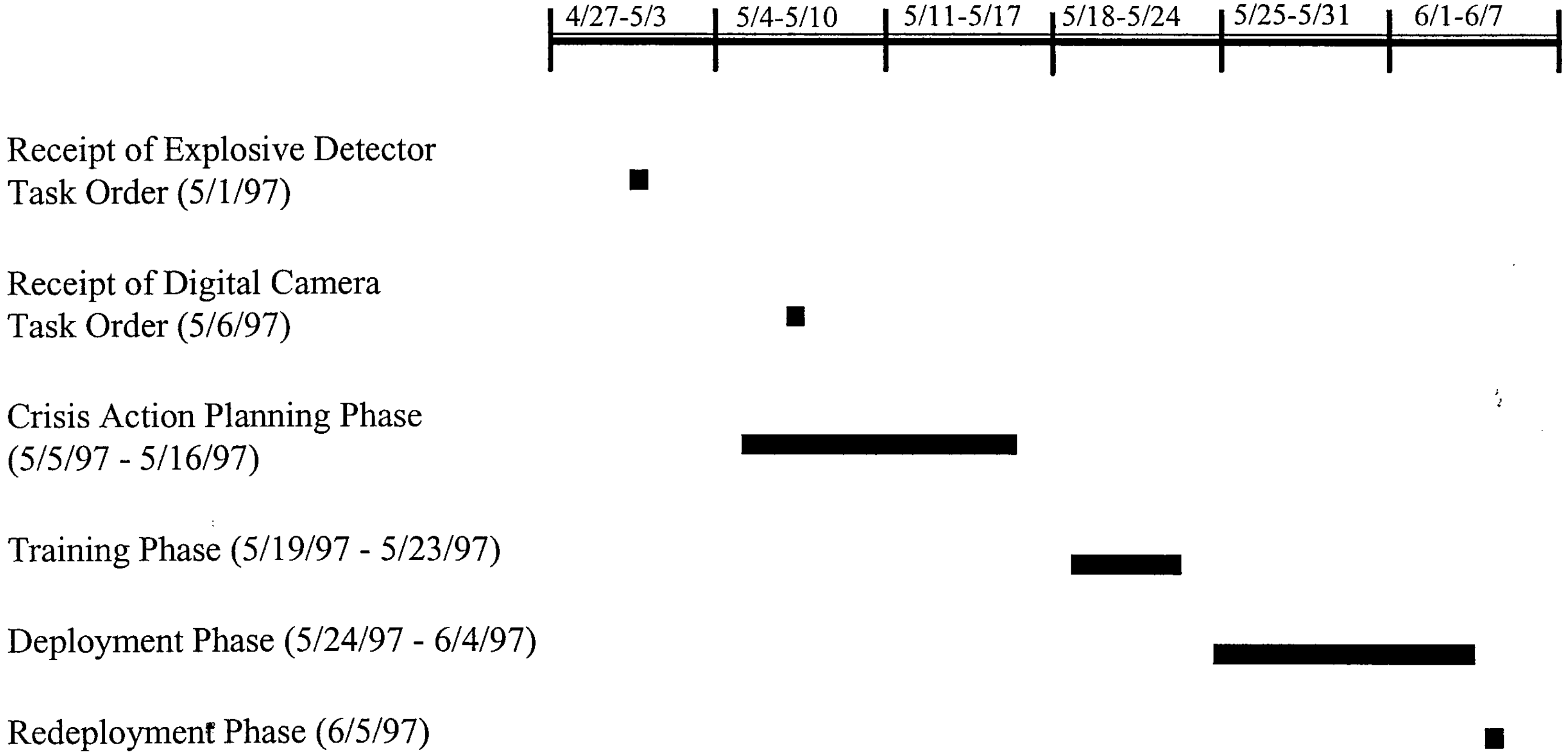
Report Period (days):	7	IONSCANS:	6	Samples/IONSCAN	1340.0	Alarm Rate (%): 0.0124
# of Days:	7	Samples/Day	1148.60	Samples/IONSCAN/Day	191.43	
Average Operational Day (hours):	23.64	Samples/Hour	48.58	Samples/IONSCAN/Hour	8.10	

COTS TESTING AND EVALUATION

MISSION

Deploy the ***COTS*** equipment requested by J-34 via Military Airlift Command (MAC) from Dover, AFB enroute to the CENTCOM AOR in order to equip and train service members assigned to Southwest Asia (SWA) in the use of the Barringer IONSCAN Model 400 (explosive detector); on order redeploy via commercial air.

COTS TIMELINE



Receipt of Explosive Detector Task Order (5/1/97)

Receipt of Digital Camera Task Order (5/6/97)

Crisis Action Planning Phase (5/5/97 - 5/16/97)

Training Phase (5/19/97 - 5/23/97)

Deployment Phase (5/24/97 - 6/4/97)

Redeployment Phase (6/5/97)

* *From receipt of the initial Task Order to units trained in the field = 20 working days*

SWA UNITS FIELDED

- 4404th SPS - USAF/Prince Sultan Air Base
- 4406th SPS (Al Jabbar) - USAF/Kuwait
- 4409th SPS (Al Eskan Village) - USAF/Riyadh
- AMPRO - USA/Kuwait
- HQ ARCENT - USA/Dhahran
- Science Advisor - USN/Bahrain

OPERATIONAL TESTING

- Environment presented unique challenges
- Sand is extremely fine in SWA (similar to talcum powder or flour)
- Manufacturer developed improved filters
- Heat (Barringer specs the Ionscan to between 32°F and 104°F)
- Temperatures in SWA routinely exceed 115°F in the shade

DATA COLLECTION EFFORT

- Formulates the basis for "Lessons Learned"
- Fielded unit should not be burdened with this responsibility
- Effort should be carried out by a contractor or some other agency
- Effort should be rotated from site to site where ever there is a piece of equipment deployed
- Focus should be "trends" at different sites

LOGISTICAL SUPPORT

- Troubleshooting
- Faulty parts covered under warranty for 12 months
- Minimum downtime
- Other real world concerns

SUSTAINMENT TRAINING

- Personnel turbulence in SWA is very high
- Knowledge of the Ionscan is “use or lose”
- Resident experts depart with skill
- Training base is quickly lost
- Sustainment training is critical to the success of a “high tech” solution similar to the Ionscan

SUCCESSES

- Computer Based Training (CBT on a CD ROM)
- Troubleshooting from a remote location
- Collection of parametric data

CONCLUSIONS

- Operational testing will validate capabilities of COTS equipment
- Data collection effort will strengthen the argument for additional equipment
- Logistical support and sustainment training could make the difference between success and failure
- No single technological solution exists to adequately screen vehicles or personnel for explosive devices

New Dimensions in Security Threats and Countermeasures

Leopold L. TARGOSZ, Jr.
CNO(N09N3)/NAVCRIMINVSERV
(202) 433-9138 ltargosz@ncis.navy.mil

THE CHANGING WORLD

IN THE PAST TEN YEARS

- Defense budget cut by 40%
- Armed forces reduced by 36%

THE CHANGING WORLD

NATURE OF THE MISSION

- Peacekeeping
- Disaster response
- Humanitarian assistance
- Drug interdiction

THE CHANGING WORLD

EVOLVING THREAT

- Preeminence of the United States
- Asymmetrical threat
  - Global
  - Poorly defined

"…the military is being called on to do more than ever. Today's armed forces, particularly the Navy and Marine Corps, have been called on to respond to crises at a rate three times greater than during the Gulf War years."

John H. Dalton

PARADIGM SHIFT

PHYSICAL SECURITY FOCUS

- Asset Protection
- Acquisition System Protection
- Force Protection

FORCE PROTECTION VISION

NAVY'S THRUST AREAS

- Maximize Indications and Warnings (Ops and Intel fusion)
- Ensure forces ashore and afloat capable of limited self-defense
- Exploit ***security technology***

SECURITY TECHNOLOGY

ENGINEERING APPROACH

- Improve regional C2 … to allow for rapid response and reinforcement capability
- Deploy portable systems … to enhance shipboard, waterfront, and installation security posture
- Integrate and consolidate security systems to absorb infrastructure reductions

SECURITY TECHNOLOGY

RDT&E STRATEGY

- Emphasize near-term integration of COTS components
- Demonstrate “cutting-edge” systems at operational sites
- Focus attention on human factors, reliability, and maintainability

SECURITY TECHNOLOGY

RDT&E FORUMS

- Physical Security Equipment Action Group (PSEAG)
- Technical Support Working Group (TSWG)

SECURITY TECHNOLOGY

PSEAG

- Oriented to military services
- Formalized requirements definition process
- Delineated areas of responsibilities
    - Explosive detection
    - Shipboard and waterfront security
- Stabilized funding levels

SECURITY TECHNOLOGY

TSWG

- Oriented to “government-wide” customers
- Annualized business cycle
- Focused on rapid research, development, and prototyping
  - Entry point screening
  - Blast mitigation

Personnel Identification System Utilizing Low Probability of Intercept Techniques for Covert Operations

David J. Chiang
U.S. Army CECOM-NVESD
AMSEL-RD-NV-SR-R, Fort Monmouth, NJ 07703-5206

Michael C. Zari, Chris S. Anderson, Anthony F. Zwilling, Joe W. Fikes
Dynetics, Inc.
1000 Explorer Blvd, Huntsville, AL 35806-2800

David A. Hess, Reeder N. Ward
Harris Corporation
P.O. Box 98000, Melbourne, FL 32902-9800

ABSTRACT

This paper documents the design of a Laser / RF Personnel Identification (ID) System developed by the US Army CECOM and the Dynetics Corporation. The ID System includes an eye safe Laser Interrogation Unit with a programmable activation code. The Interrogation Unit is very directive for low probability of intercept (LPI) which is of interest during covert operations. A Responder Unit is worn by the soldier and transmits a LPI RF response centered at 900 MHz, only after receiving the proper interrogation code. The basic subsystems for the identification system are a Laser Interrogation Unit, a RF Responder Unit, and an electronic Programming / Synchronization Unit. The operating principles for the subsystem are reviewed and the design issues are discussed. In addition to the design performed under Phase I of the program, a breadboard system was developed to validate the proof of principle concept. Hardware implementation is reviewed and field testing of the breadboard is presented. The Phase II development, engineering plans, and preliminary results are also presented.

The military application of this system is evident through the official reports of fratricide experienced both in the Gulf War and more recently, in military overseas operations in countries with heavily armed indigenous inhabitants. Fratricide represents an unacceptable political risk for US peacekeeping operations. Military users of the system potentially include all ground based as well as some other combat forces. Other military and civilian users will depend on the Laser / RF Identification technology being developed under the current Phase II effort. This includes the Dual-Use need for a long range (1-km), highly reliable, non-voice, and non-spatial resolution based ID technique for restricted area protection. Commercial users would benefit from this dual use development in the areas of law enforcement, motor vehicle identification, and intrusion systems. As an example of the concept's versatility, the system can be applied commercially in law enforcement to perform remote vehicle identification without visual contact with the license plate number.

Although their applications differ drastically, military and commercial users require similar product features, indicating a need for increased manufacturing and lower costs. The development of the laser interrogator with a RF response is a low cost solution to extremely important security issues.

1. SYSTEM CONCEPT AND PRELIMINARY SPECIFICATIONS

Figure 1 illustrates the *Soldier Identification System* concept. In operation, the Interrogation Unit transmits a highly directive, encoded laser burst to an unknown person (ie target) at ranges in excess of 2 km. Simultaneously, a spread spectrum RF code is transmitted by the Interrogation Unit for additional verification and security. The Responder Unit detects both the modulated optical and RF signals. Upon verification that a valid interrogation has been made, the Responder Unit transmits a low probability of intercept (LPI) spread spectrum RF response.

The Interrogation Unit expects a response during a specified time window. Upon verification that a valid RF response has been received, indicators (both audio and tactile) on the Interrogation Unit alert the gunner to the status of the interrogation. The interrogation and response codes are programmable to allow for "code of the day" operation, and the codes can be changed automatically at, for example, 12 hour intervals in all Interrogation and Responder Units. This feature helps defeat undesirable playback of captured codes.

Table 1 lists the operational specifications for the *Soldier Identification System*. Operating platforms are given for the Interrogation Unit, and the designed platform for the Responder Unit is the field soldier. Since power, size, and weight were minimized during design, the Responder Unit can be easily adapted to vehicle platforms, ie. Armored personnel carriers (APCs). Characteristics for the Prototype Interrogation are shown in ***Figure 2***. As noted in the figure, the prototype system includes visible and infrared aiming lasers compatible with Army nightvision devices. It should be noted that the aiming lasers are not required for the interrogation function.

Table 1. Prototype Soldier ID Specifications

Parameters	*Prototype Specifications*
Maximum Range ID (P=0.90 %)	2000 meters
Minimum Range ID (P=.0.90 %)	0.25 meters
Interrogation Angular Resolution * (mrad)	10
Maximum Interrogation Time (sec)	1.0
Eyesafe Operation of Laser	Yes
Low Probability of Intercept (LPI)	Yes
Day / Night Operation	Yes

*Note: Angular Resolution can easily be modified to suit operational requirements.

2. PROTOTYPE DESIGN ISSUES

2.1 Interrogation Unit

Key subsystem components of the Interrogation Unit include the laser transmitter, the spread spectrum RF transceiver, code processor/controller, and the interrogation activation switch. To meet the goals/requirements for this interpersonnel communication system, many design issues have been addressed, including the selection of laser characteristics (wavelength, beam size, and power), interrogation code generation for LPI, and RF transmitter and receiver characteristics that meet LPI, range, and low power consumption requirements.

2.1.1 Optical Considerations

During an interrogation cycle, the interrogation laser diode is modulated with a specific code, which in turn causes the laser diode to emit laser light in the same code. The light is radiated from the laser diode typically at a high divergence angle (ie. 40 degrees) and must be collimated by a lens to the divergence required for achieving operational resolution. Thus, the laser diode and lens assembly produces a nearly collimated (ie. 10 mrad divergence) optical beam that is used to optically interrogate the target.

There were many key considerations in designing the optical system, including wavelength selection of the interrogation laser, eye safety, optical power to meet system range requirements, laser diode output characteristics, availability of commercial off the shelf components (COTS), and operational environment. Solar radiation about the interrogation laser wavelength, and the detection of the optical interrogation signals by current nightvision equipment were also considered.

A design spreadsheet was developed to compare performance tradeoffs between different optical system component combinations. The spreadsheet includes inputs on the laser parameters, interrogation code specifics, the system operational scenario, and optical receiver parameters. Calculations include signal levels at minimum and maximum ranges, contributions due to solar irradiance, signal variations at range limits, receiver noise terms, and the potential signal to noise ratio (SNR) (at maximum range) based on single pulse detection. In addition, eye safety calculations are performed in the spreadsheet based on code duration, wavelength, power, etc. These calculations are used to determine if the laser interrogation follows ANSI standards for eye safety and maximum permissible exposure (MPE).

2.1.2 RF Considerations

In addition to the laser interrogation code, a second interrogation code is modulated and transmitted from the Interrogation Unit to the Responder Unit via a RF transmitter. In this sense, the RF code provides an omnidirectional interrogation. For this dual mode laser/RF *Soldier Identification System*, the laser portion of the interrogation system provides directional selectivity while the RF interrogation provides additional security. Note that directionality of the RF interrogation can be achieved at the expense of increased size, weight, and cost.

As with the optical system, there are many considerations in designing the RF system, including frequency selection, RF power to meet system range requirements, LPI considerations, availability of COTS components, and operational scenario. Desirable features for the RF transceiver system include compact size, low power consumption, battery operation, reprogrammability, and sleep mode operation.

Given the operational environment and requirements placed on the system, spread spectrum technology has been selected for the prototype *Soldier Identification System* testing and demonstration. The spread spectrum modulation scheme for the RF portion of the communication system provides LPI of the interrogation/response codes in addition to interference rejection/suppression of both environmental and intentional sources. For the prototype system development, a frequency hopping, spread spectrum (FHSS) modulation scheme was utilized.

2.1.3 Weapon and User Interfaces

For the prototype *Soldier Identification System*, the Interrogation Unit mounts to the weapon (ie. M16-A2 platform) with the scope mount attachment. The weapon interface was designed so that the gunner can still use the M-16 weapon's metal sights for aiming. As mentioned, the attachment interface to the M-16 weapon can be modified to meet the application requirements. Interfaces are required for initiation of an interrogation cycle and to indicate the results of the interrogation to the gunner. Considerations for the interfaces include the system operational environment and ergonomics. A pressure switch located on the lower hand guard of the M19-A2 rifle activates the interrogation cycle. The individual gunner to suit ergonomic considerations can adjust the location of the switch. For the prototype *Soldier Identification System*, both audible and vibration indicators alert the gunner to the status of the interrogation. The selected indicator will have an output only if a "friend" response has been verified. An "unknown" response will be noted by the lack of an indicator output.

2.2 Responder Unit

At the Responder Unit, an optical detector assembly is used to detect the laser interrogation code. In addition, a RF transceiver is used to receive the RF interrogation code. When both of the received codes match the stored reference codes, an RF response code is sent from the Responder Unit. The RF response code will be transmitted via the FHSS transceiver on the Responder Unit. Back at the Interrogation Unit, the response code is detected and compared to the stored reference code for the proper response. Once the received RF code has been verified as a valid response, a signal is sent to the indicators (ie. LED and/or vibrator) on the Interrogation Unit indicating a "friend".

The Responder Unit is small, lightweight, and attaches to the soldier's uniform. The operation of the Responder Unit is completely transparent to the soldier or end user.

The transmitted interrogation signal is received via the infrared (IR) detectors that are attached to the soldier's uniform to provide a complete hemispherical field of view (FOV). The filtered detector package is connected to the optical front end portion of the Responder Unit via shielded cable. Design issues for the Responder Unit are similar to those of the Interrogation Unit with the additional requirement of withstanding the expected environment of the platform – the individual soldier in combat or training situations.

3. PROTOTYPE TESTING

Figure 4 shows the Prototype Interrogation Unit on a M16 platform. Key components, such as the interrogation laser/optics, FHSS transceiver, activation switch, and "friend" indicator are identified in the figure. Also noted in the figure are the end user boresight adjustments to align the prototype system with the weapon's metal sights. **Figure 5** shows the prototype Responder Unit components and the prototype system housed in a vest for prototype *Soldier Identification System* testing. Testing of the prototype *Soldier Identification System* was performed at the U.S. Army Infantry Center (USAIC) Dismounted Battlespace Battle Lab (DBBL) in Ft. Benning, Georgia, and at the Redstone Technical Test Center (RTTC) in Huntsville, Alabama.

3.1 Testing at USAIC DBBL

Prototype testing was performed at the DBBL (Figure 6) as part of the Concept Evaluation Program (CEP). A major objective of the CEP tests was to determine the performance parameters, under both benign and realistic conditions, of candidate combat identification (CID) technologies. The performance parameters evaluated during the test were based on a subset of the Combat Identification for Dismounted Soldiers (CIDDS) Operational Requirements Document (ORD) required capabilities. Parameters measured include probability of correct identification, interrogation resolution, and timeliness.

Testing was performed by the Government at Buckner Range and at Decker Strip at Ft. Benning, GA, under day and night conditions. Testing was performed at ranges out to 1375 meters which was the maximum line of sight (LOS) range available for the system testing. In addition, testing was performed with the gunner (Interrogation Unit) and target (Responder Unit) in various configurations and scenarios. Scenarios included the gunner in a stationary position (ie. Standing or prone) and target in either a stationary position (ie. Standing, kneeling, or prone) or moving (ie. Running through a wooded area). For the testing, the gunner aims the weapon and proceeds to interrogate the target a set number of times per each position. Data collection occurred for each set of tests, as shown in **Figure 6**. In addition, each set of tests was repeated with different personnel/gunners performing the interrogations. Also for the night tests, aiming of the Interrogation Unit was assisted by the IR aiming laser on the prototype system and with the use of night vision devices.

The *Soldier Identification System* prototype demonstrated a 90% probability of correct identification. The system was successfully tested during both day and night conditions out to the maximum available range of 1375 meters.

3.2 Testing at RTTC

Performance testing was also performed at the Redstone Technical Test Center (RTTC). The major objective of these tests was to determine range performance of the prototype system; to determine the probability of correct identification as a function of range. For the tests, the Interrogation Unit was mounted on a tripod and the Responder Unit was moved to various locations on the test area. For each test, the target remained in the standing position and was interrogated a set number of times, and the number of valid responses were noted. Based on the testing, the prototype *Soldier Identification System* was successfully tested to ranges in excess of 4000 meters. At a range of 3500 meters, the system successfully achieved a 90% probability of correct identification.

4. CONCLUSION

In summary, the prototype *Soldier Identification System* has resulted in a very compact, cost-effective solution that meets the dismounted soldier identification requirement. The innovative laser/RF concept feasibility was determined through design and simulation, and demonstrated through prototype system testing. Advantages of this approach include low cost, LPI, potential for range extension, and fast (<600 msec) interrogation decision times. The prototype *Soldier Identification System* was made available to the Government (USAIC DBBL) for evaluation by the military community under various combat test conditions. As a result of the extensive testing, the performance of the system surpassed the anticipated performance, achieving a 90% correct probability of identification to a range of 3500 meters.

REFERENCES

1. "New Electronic Device Developed to Prevent Friendly Fire Incidents", *Defense Electronics,* p. 12, March 1995

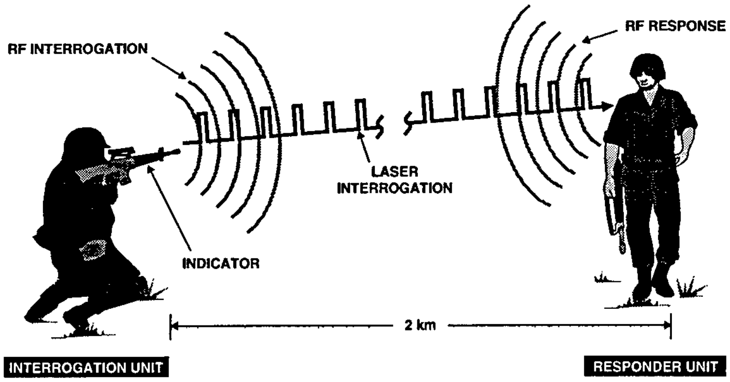
2. Cornelius, G., "U.S. Forces Seek Affordable Solutions to Combat Identification Problems", *Signal,* p. 71-73, September 1994.

3. "Joint Operational Requirements Document for the Combat Identification System".

4. "American National Standard for the Safe Use of Lasers", ANSI-Z136.1-1993.

5. Holmes, J.K., *Coherent Spread Spectrum Systems,* John Wiley & Sons, New York, 1982

6. Dixon, R.C., *Spread Spectrum Systems,* John Wiley & Sons, New York, 1982



TR-97-0466-NC

Figure 1. Laser/RF Soldier Identification System Concept

INTERROGATION UNIT

- DIRECTIONAL LASER TRANSMITTER (EYESAFE, LPI)
- OMNIDIRECTIONAL RF TRANSCEIVER
- LPI SPREAD-SPECTRUM INTERROGATION
- INDICATOR FOR INTERROGATION RESULTS
- END-USER BORESIGHT ADJUSTMENTS
- LOW-BATTERY INDICATOR
- REPROGRAMMABLE VIA RF LINK
- VISIBLE (RED) AIMING LASER* (EYESAFE)
- IR AIMING LASER* (EYESAFE)

RESPONDER UNIT

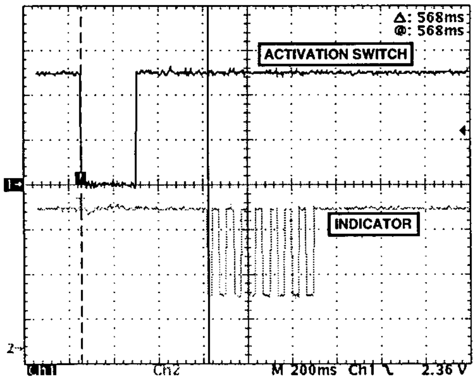
- LASER DETECTORS/RECEIVER
- OMNIDIRECTIONAL RF TRANSCEIVER
- LPI SPREAD-SPECTRUM RESPONSE
- PROTOTYPE DEVELOPED FOR DISMOUNTED SOLDIER APPLICATION
- REPROGRAMMABLE VIA RF LINK

DAY/NIGHT OPERATION

*NOT REQUIRED FOR INTERROGATION FUNCTION

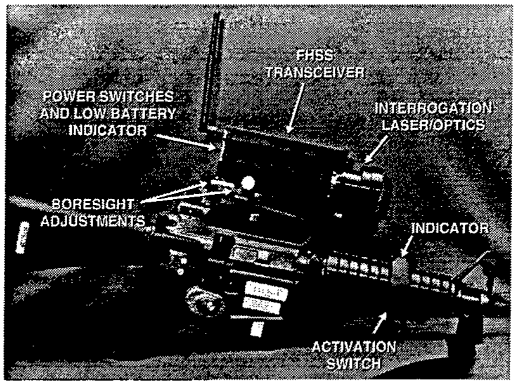
TR-97-0467-NC

Figure 2. Prototype "Solder Identification System" Characteristics



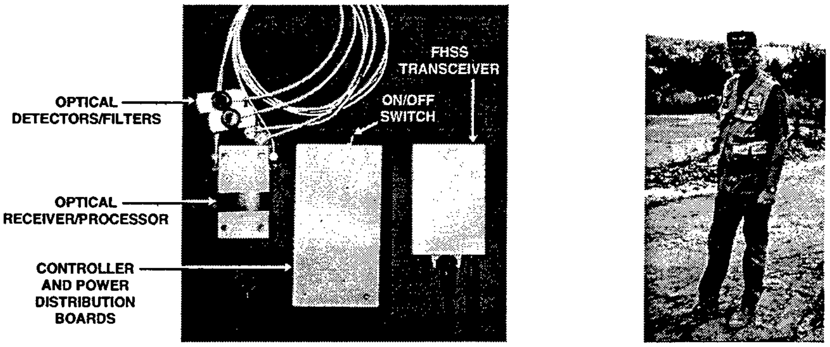
TR-97-0468-NC

Figure 3. Breadboard Testing: Closed-Loop Interrogation Times


FHSS TRANSCEIVER
POWER SWITCHES AND LOW BATTERY INDICATOR
INTERROGATION LASER/OPTICS
BORESIGHT ADJUSTMENTS
INDICATOR
ACTIVATION SWITCH

TR-97-0469-NC

Figure 4. Prototype Interrogation Unit on M16 Platform


FHSS TRANSCEIVER
OPTICAL DETECTORS/FILTERS
ON/OFF SWITCH
OPTICAL RECEIVER/PROCESSOR
CONTROLLER AND POWER DISTRIBUTION BOARDS

(a) Components **(b) Vested-Housed Prototype**

TR-97-0470-NC

Figure 5. Prototype Responder Unit

TR-97-0471-NC

Figure 6. Prototype "Soldier Identification System" Testing at DBBL

TEST AND EVALUATION OF PANORAMIC IMAGING SECURITY SENSOR FOR FORCE PROTECTION AND FACILITY SECURITY

Session VIII B: Physical Security Technologies

Daniel A. Pritchard, Robert L. White, Douglas G. Adams, Erik Krause, Eric T. Fox,
Mark D. Ladd, Richard E. Heintzleman, Patricia C. Sprauer

Sandia National Laboratories
PO Box 5800
Albuquerque, NM 87185-0780

505-844-7444 Voice
505-844-5569 Fax
dpritch@sandia.gov

John J. MacEachin
Raytheon Systems Company
1300 MacArthur Blvd.
Mahwah, New Jersey
07430-2052
201-327-7700

MacEachin@ecd-hac.com

TEST AND EVALUATION OF PANORAMIC IMAGING SECURITY SENSOR FOR FORCE PROTECTION AND FACILITY SECURITY

Daniel A. Pritchard, Robert L. White,
Douglas G. Adams, Erik Krause, Eric T.
Fox, Mark D. Ladd, Richard E.
Heintzleman, Patricia C. Sprauer
Sandia National Laboratories
Albuquerque, NM 87185-0780

John J. MacEachin
Raytheon Systems Company
1300 MacArthur Blvd.
Mahwah, New Jersey
07430-2052

ABSTRACT

This paper describes the design and preliminary test results of a 360-degree scanning, multi-spectral intrusion detection sensor. This moderate-resolution, panoramic imaging sensor is intended for exterior use at ranges from 50 to 1500 meters. This Advanced Exterior Sensor (AES) uses three sensing technologies (infrared, visible, and radar), separate track processors and sensor fusion to provide low false-alarm intrusion detection, tracking, and immediate visual assessment. The images from the infrared and visible detector sets and the radar range data are updated as the sensors rotate about once per second. The radar provides range data with one-meter resolution. This sensor has been designed for low-cost, easy use and rapid deployment to cover wide areas beyond, or in place of, typical perimeters, and tactical applications around fixed or temporary high-value assets. A prototype AES has been developed and preliminary test results are presented. This sensor represents a growing trend to use low-cost thermal imaging sensors, combined with other devices and advanced processing, for protection of U.S. military forces and other national assets.

INTRODUCTION

The Advanced Exterior Sensor (AES) is an intrusion detection and tracking system for wide area coverage in ground-based security applications. The requirements are to detect human and vehicle intrusions across various terrain and environmental conditions. It has been designed to be rapidly deployable and simple to set up and operate, and suitable for both day and night operations.

The AES integrates three sensor technologies (thermal infrared waveband, visible waveband, and microwave radar) with three motion detection target trackers and a sensor fusion software module to achieve higher performance than single technology devices. Wide areas are covered by continuously scanning the three sensors 360 degrees in about one second. No commercial-off-the-shelf (COTS) system exists today that combines these technologies.

Sensors capable of wide area, stand-off intrusion detection are gaining increased importance in applications ranging from upgraded fixed perimeter security to rapid-deployment force protection on peace-keeping missions. Adding imaging and motion detection capabilities to wide area sensors enhances their usefulness and provides the operator immediate visual alarm assessment.

Video motion detection (VMD) systems have been applied primarily to closed-circuit television (CCTV) cameras around perimeters; however, recent evaluations show

* This work was sponsored by the Defense Special Weapons Agency. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

nuisance alarms are still high [Ringler-95], and most applications have focused on clear zones, not unstructured areas. The AES project was designed to include VMD by capitalizing on faster processors and advanced detection and tracking algorithms. One goal of the AES project is to combine these in an affordable package.

Design Requirements for an Advanced Exterior Sensor

At the beginning of the *AES* project, the following general requirements for a stand-off intrusion detection sensor were identified:

1. Capable of wide area coverage (hundreds of meters for humans and vehicles).
2. Detection and tracking of multiple targets.
3. Capable of detecting a wide range of penetration scenarios.
4. High probability of detection (Pd).
5. Low nuisance alarm rate by discriminating humans and vehicles from nuisance sources.
6. Capable of 24-hour operation in varying environmental and climatic conditions.
7. Limited mechanical moving parts.
8. Capable of sectorized assessment while maintaining detection in the remaining areas.
9. Passive (low electromagnetic signature).
10. Low life-cycle cost.

Additional requirements and clarification of these parameters were derived from related programs, interviews with individuals in the security field, operational requirements documents, and other agencies and sources.

Specific Design Parameters

The *AES* was designed to detect and track humans and vehicles in accordance with the ranges summarized in Table 1. Targets moving as slowly as 0.25 meter per second (0.1 m/sec desired) are to be detected as well.

The *AES* was designed to reduce nuisance alarms based on motion of the objects. The *AES* detects motion in a full 360° while assessing alarms from other locations by continuous azimuth scanning. The system can accommodate uneven terrain by varying the elevation angle during rotation, but this has not yet been fully implemented.

Initial detection and tracking performance, as described later, is meeting expectations and any refinements to the infrared sensor will result in overall system improvements.

Table 1. Detection range requirements.

Target	Conditions	Range (req'd)	Range (desired)
Upright human walk/run 0.6x1.65 m 1.0 m^2	Clear, good visibility	500 m	750 m
	Light rain, humid	350 m	525 m
Crawling human head-on 0.5x0.3 m 0.15 m^2	Clear, good visibility	250 m	375 m
	Light rain, humid	200 m	300 m
Truck/van 1.5x1.5 m 2.3 m^2	Clear, good visibility	1000 m	1500 m
	Light rain, humid	800 m	1200 m

Components of the AES

The *AES* consists of three major components. The Remote Sensor Module (RSM), shown in Figure 1, is a rotating sensor pod that is placed in the field and remotely connected over a high-speed data link to a high-speed Data Processing Module (DPM). Eventually, multiple RSMs and DPMs (used in combination) can be networked to cover a very large facility. A single Display Control Module (DCM) is used to configure and control an RSM and DPM.

Remote Sensor Module

An infrared sensor was selected to provide good quality imagery in both day and night conditions, with some advantage during poor weather as well. A lead-selenide (PbSe) linear infrared array, operating in the 3-5 micron thermal infrared band, was selected as the primary sensing device in the ***AES*** RSM.

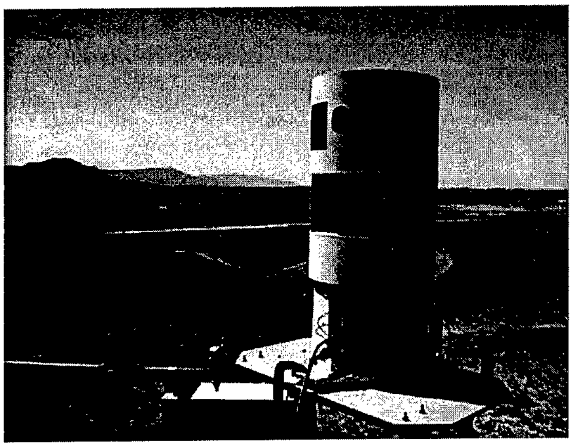


Figure 1. Remote Sensor Module

Performance modeling of the system using a 160-element PbSe linear array predicted the Minimum Resolvable Temperature Difference curve shown in Figure 2 [see also Pritchard-94]. Also shown in this figure are measured MRTD values taken before and after some system refinements, including detector replacement and focus adjustments. Performance of the infrared sensor is not as good as predicted, however, and some additional investigations are under way.

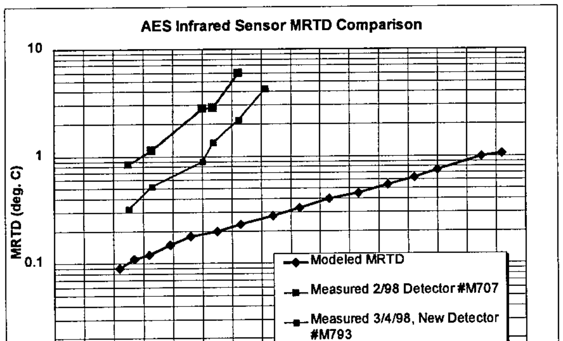


Figure 2. AES MRTD Comparison

A visible-waveband imaging sensor and a microwave radar sensor were chosen to complement the infrared sensor. The visible band sensor effectively supplements the limitations of an infrared sensor during periods of low thermal contrast in warm background, daytime operation. A radar has been included to overcome rain and fog obscuring the infrared sensor. The radar developed for the ***AES*** is a frequency modulated, continuous wave (FMCW) radar with area moving-target indication (AMTI). The chosen frequency (17 GHz) was based on rain clutter and human signature modeling. Additional details of the system are described in [Garcia-97].

Data Processor Module

The DPM (Figure 3) consists of an industry-standard VME backplane and industrial quality enclosure, a custom Fibre Channel receiver and demultiplexer board, a high-speed PowerPC-based control computer, and two, dual Texas Instruments 320C80 digital signal processors.

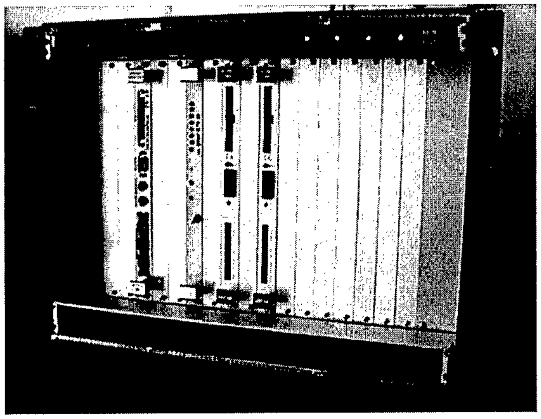


Figure 3. Data Processor Module

The ***AES*** infrared and visible motion detection (segmentation) software was based on an adaptation of the spatio-temporal constraint equation technique [Munno 93]. The radar digital signal processing is primarily 4096-point fast Fourier transform (FFT) operations with some additional infinite-impulse response filtering. The tracking software uses the output of the basic motion detection software; then *feature-based* sensor fusion software is used to combine the outputs of the three trackers to achieve an overall confidence value of the detection [Nelson-96].

DISPLAY AND CONTROL MODULE

A personal computer is used as the DCM in the ***AES.*** The special requirements are that it have an ethernet port for communication to the networked DPM suitable display for gray-scale imagery with color overlays. Although not implemented for the proof-of-concept system, the DCM will eventually have the capability to connect to and control multiple sensor modules and display imagery from each. Figure 4 shows a sample PC screen displaying a 10-degree wedge of the full 360-degree image. The image is from the visible sensor at an angle of 222 degrees from north. A truck was detected at 640 meters.

APPLICATIONS

Figure 5 shows a possible ***AES*** application with four sensor modules at each corner of a one square-kilometer protected area covering an excess of one square mile.

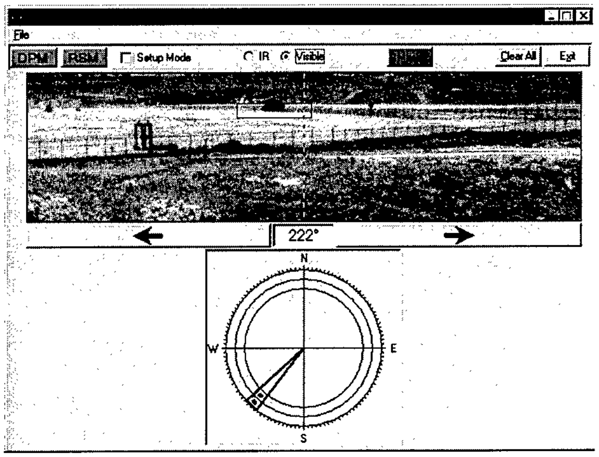


Figure 4. Sample AES DCM Screen

Many other configurations can be conceived using multiple RSMs, depending on the local site requirements. For small applications, two units can be deployed to capitalize on the ability to overlap coverage and protect a site up to 300 meters on a side. For large rectangular sites, such as runways, six units could be deployed.

PRELIMINARY AES TESTING

VEHICLE DETECTION

Preliminary testing to detect vehicles moving within the field of regard has been completed. Vehicles have been successfully tracked in several scenarios. Traffic on a freeway 4.2 km away is routinely detected and tracked. Figure 7 shows a detection of a vehicle over 4 km at night in infrared imagery. Actual detection ranges may vary depending on environmental conditions. This vehicle is beyond the range of the radar. The radar range cut-off is 1500 m. Small trucks, cars, and vans are also routinely detected and tracked on an access road to the test facility at Sandia National Laboratories.

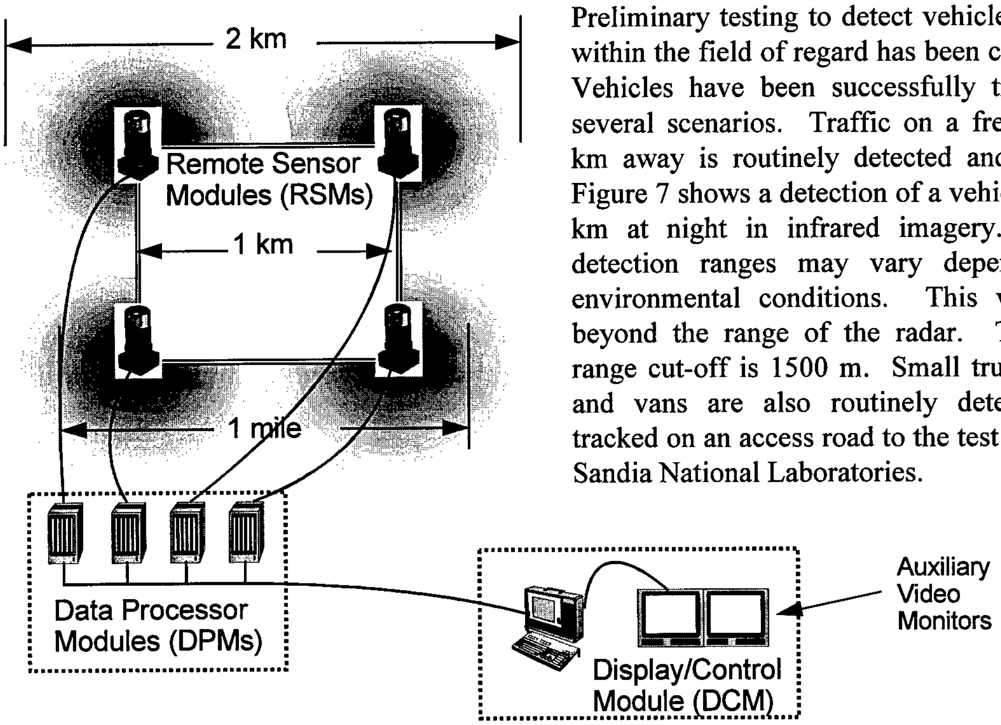

2 km
Remote Sensor Modules (RSMs)
1 km
1 mile
Data Processor Modules (DPMs)
Display/Control Module (DCM)
Auxiliary Video Monitors

Figure 5. Proposed 4-*AES* Application

Figure 6 shows a detection and track box around a vehicle at a distance of over 4 km in daytime imagery using the visible camera.

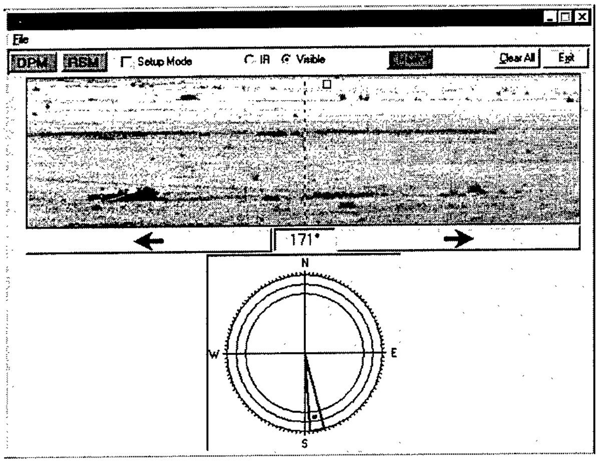


Figure 6. Vehicle Detection Over 4 km (Daytime, Visible Image)

PEOPLE DETECTION

Preliminary performance testing to detect people walking and running shows detection ranges in clear conditions of 500 m or more. Figure 8 shows detection of a person walking in a field during the day beyond 500 m. The person was detected by both the infrared and visible sensors. Figure 9 shows detection of a person at night using just the infrared sensor. This person is beyond 500 m.

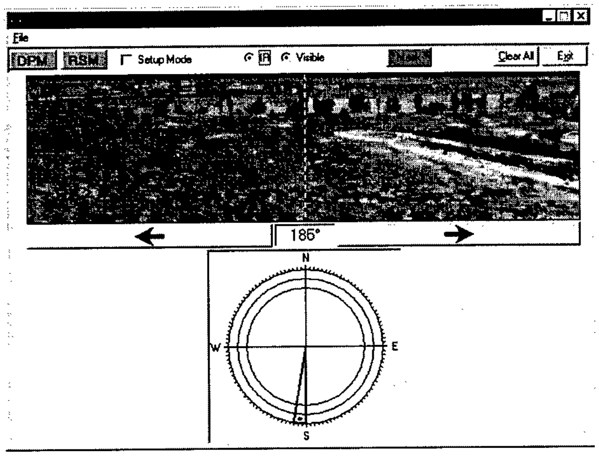


Figure 7. Vehicle Detection Over 4 km (Night, Infrared Image)

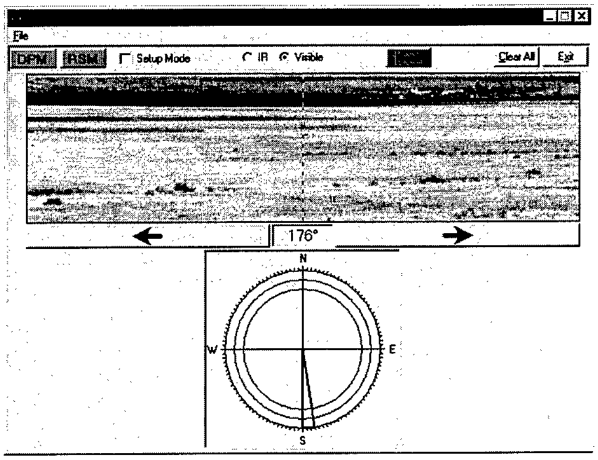


Figure 8. Detection of Person Beyond 500 m (Daytime, Visible Image)

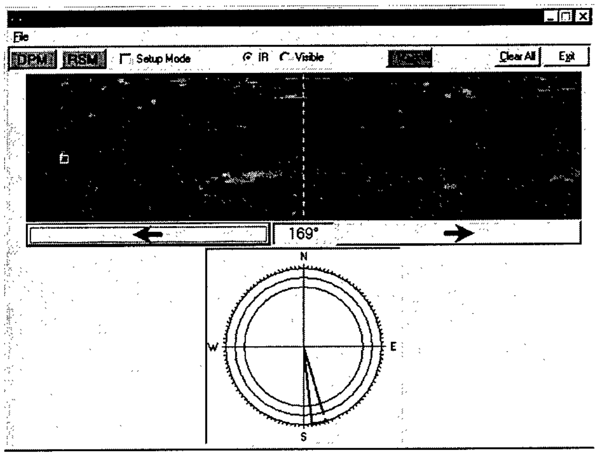


Figure 9. Detection of Person Beyond 500 m (Night, Infrared Image)

Some additional test data has been taken to detect crawlers. Figure 10 shows detection of a crawling person in the daytime beyond 250 m. The image is from the visible sensor.

Although a large amount of test data has not yet been acquired and analyzed, the results to date indicate good detection and tracking performance with the infrared and visible sensors. When the radar becomes fully operational, additional testing will be performed and detection rates are expected to increase. Some further testing will also be performed using different targets and during adverse weather conditions.

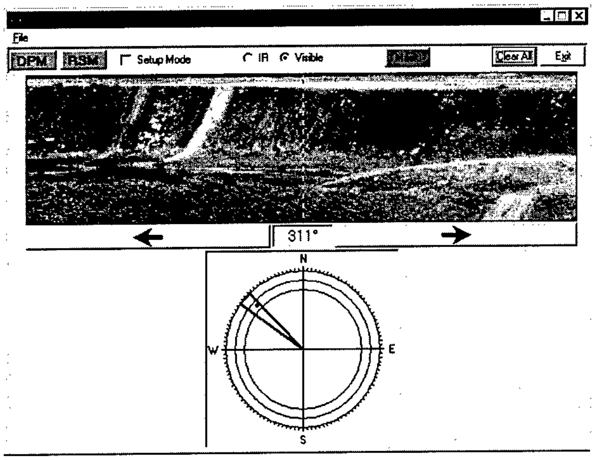


Figure 10. Detection of Crawler Beyond 250 m (Day, Infrared Image)

SUMMARY AND FUTURE EFFORTS

The ***AES*** design combines infrared imaging and visible linear arrays with an area MTI radar in a rotating sensor module. The data processor is implemented as a separate module, remotely located near the operator's display and control unit. The first operational prototype was completed in early 1998 and performance testing has begun. The system is designed to be easily deployed and be effective in many weather conditions. This is accomplished by integration and complementary processing of the signals from three discrete sensors.

Data processing requirements play a major role in the ***AES*** system design. The detection and tracking algorithms were developed to reliably detect moving objects in low signal-to-noise conditions and operate on scenes where little or no activity is expected.

Additional testing of the prototype ***AES*** will be performed to better understand the capabilities of the system to detect in various environments.

REFERENCES

Garcia-97 "Advanced Exterior Sensor," L. Garcia, D. A. Pritchard, and R. E. Burger, *Proc. 13th Annual Joint Government-Industry Security Technology Symposium*, American Defense Preparedness Association, Virginia Beach, VA, June 1997.

Munno-93 "Automatic Video Image Moving Target Detection for Wide Area Surveillance," C. J. Munno, *Proc. IEEE International Carnahan Conference on Security Technology*, 1993.

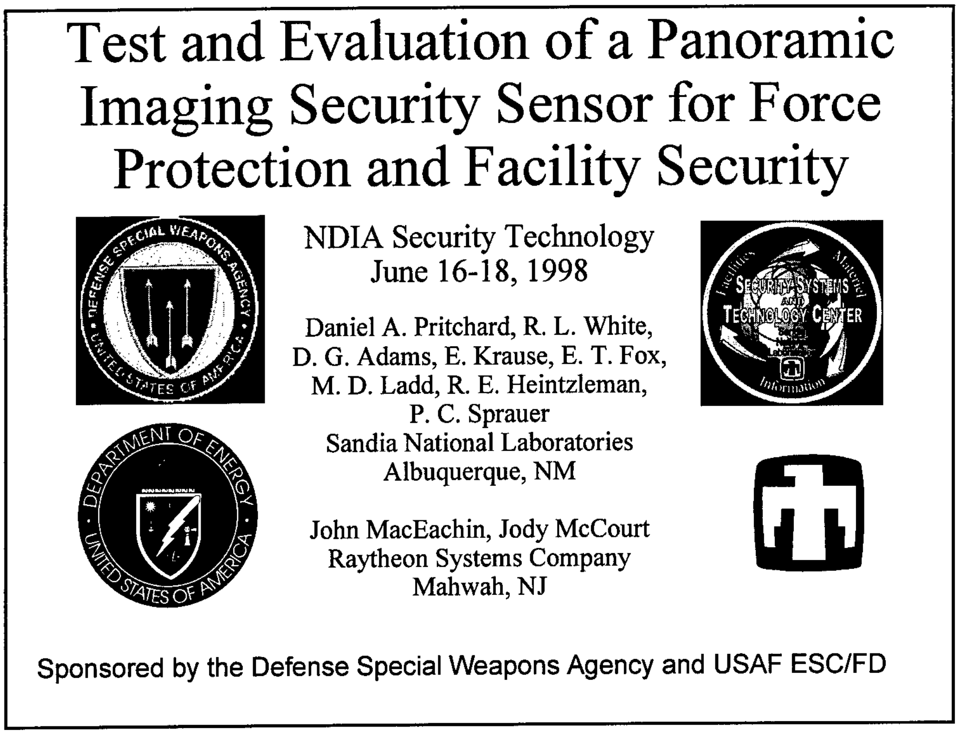
Nelson-96 "Sensor Fusion for Intelligent Alarm Analysis," C. L. Nelson and D. S. Fitzgerald, *Proc. 30th Annual IEEE International Carnahan Conference on Security Technology*, 1996.

Pritchard-93 "Evaluation of Automatic Detection of Humans and Vehicles," D. A. Pritchard, R. F. Davis, and J. E. Simpson, *Proc. IRIS Specialty Group on Targets, Backgrounds, and Discrimination*, ERIM, Ann Arbor, MI, January 1993.

Pritchard-94 "Panoramic Imaging Sensor Design and Modeling," D. A. Pritchard, *Proc. IRIS Specialty Group on Passive Sensors*, ERIM, Ann Arbor, MI, March 1994.

Pritchard-95 "System Overview and Applications of a Panoramic Imaging Perimeter Sensor," D. A. Pritchard, *Proc. 11th Annual Joint Government-Industry Security Technology Symposium*, American Defense Preparedness Association, Virginia Beach, VA, June 1995.

Ringler-95 "Evaluation of Commercially Available Exterior Digital VMDs," C. E. Ringler and C. E. Hoover, Sandia National Laboratories internal report SAND94-2875, Albuquerque, NM, June 1995.



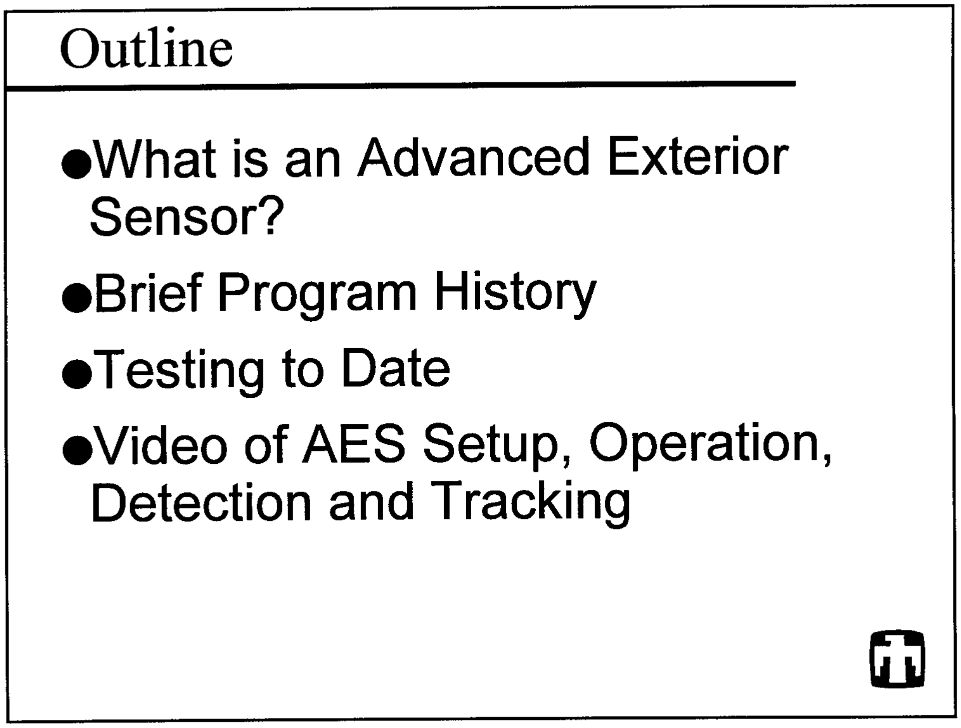
Test and Evaluation of a Panoramic Imaging Security Sensor for Force Protection and Facility Security

NDIA Security Technology
June 16-18, 1998

Daniel A. Pritchard, R. L. White,
D. G. Adams, E. Krause, E. T. Fox,
M. D. Ladd, R. E. Heintzleman,
P. C. Sprauer
Sandia National Laboratories
Albuquerque, NM

John MacEachin, Jody McCourt
Raytheon Systems Company
Mahwah, NJ

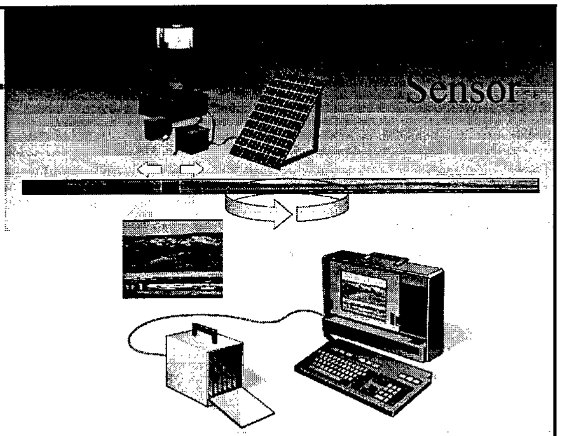
Sponsored by the Defense Special Weapons Agency and USAF ESC/FD



Outline

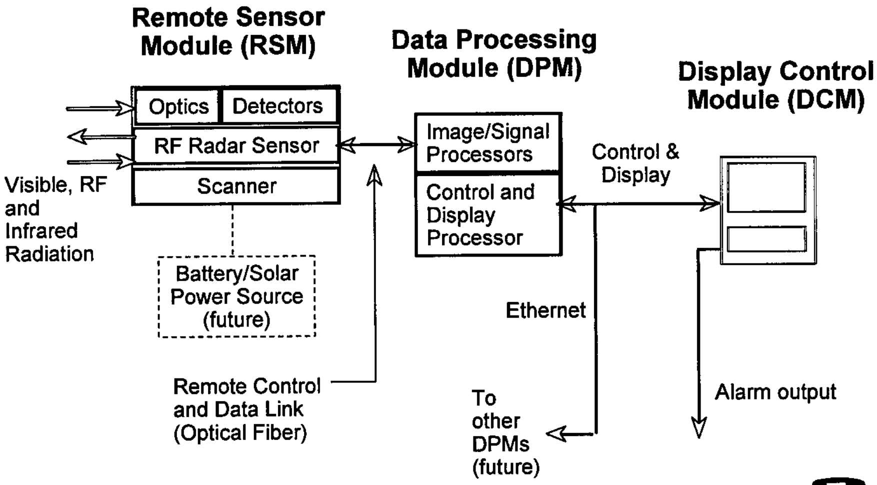
- What is an Advanced Exterior Sensor?
- Brief Program History
- Testing to Date
- Video of AES Setup, Operation, Detection and Tracking

AES is...

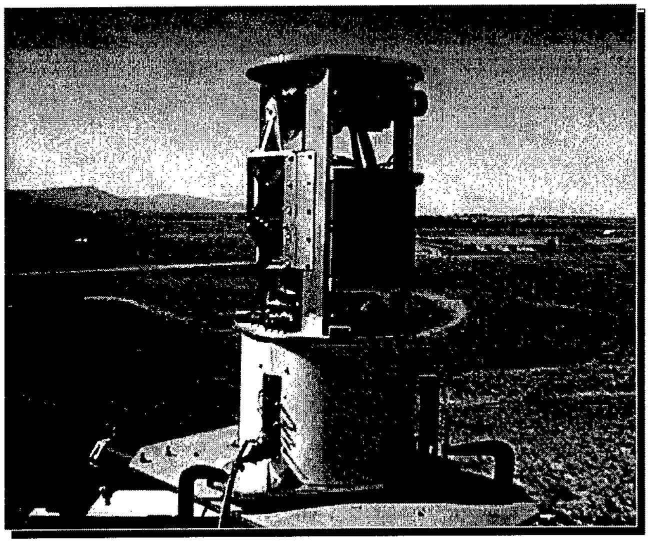


- **A sensor system**
- **Continuous 360-degree imagery**
- **3 sensors**
  - ➧ IR, Visible, Radar
- **3 target trackers**
- **Detects deliberate motion in 360 degrees**
  - ➧ People more than 500 m, vehicles more than 1500 m
- **Provides immediate visual assessment**
- **Rapidly deployed, designed for long life**

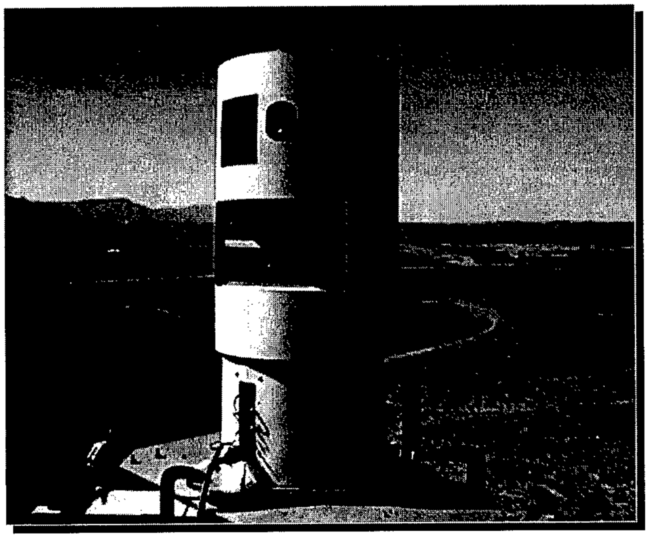
AES Block Diagram


Remote Sensor Module (RSM)
Optics
Detectors
RF Radar Sensor
Scanner
Visible, RF and Infrared Radiation
Battery/Solar Power Source (future)
Remote Control and Data Link (Optical Fiber)
Data Processing Module (DPM)
Image/Signal Processors
Control and Display Processor
Ethernet
To other DPMs (future)
Control & Display
Display Control Module (DCM)
Alarm output

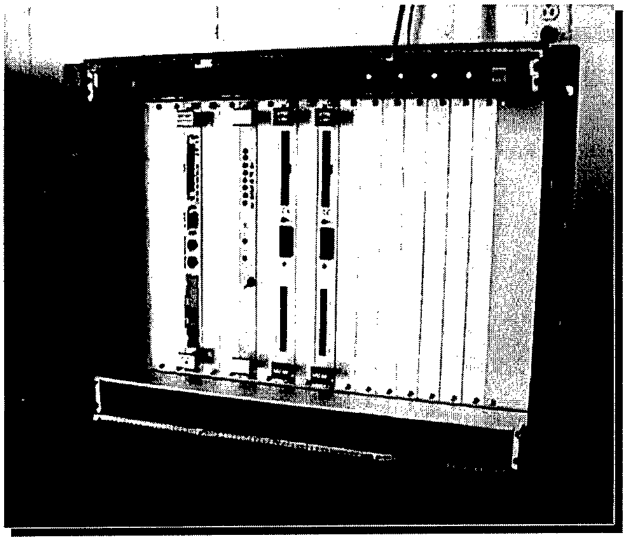
Remote Sensor Module



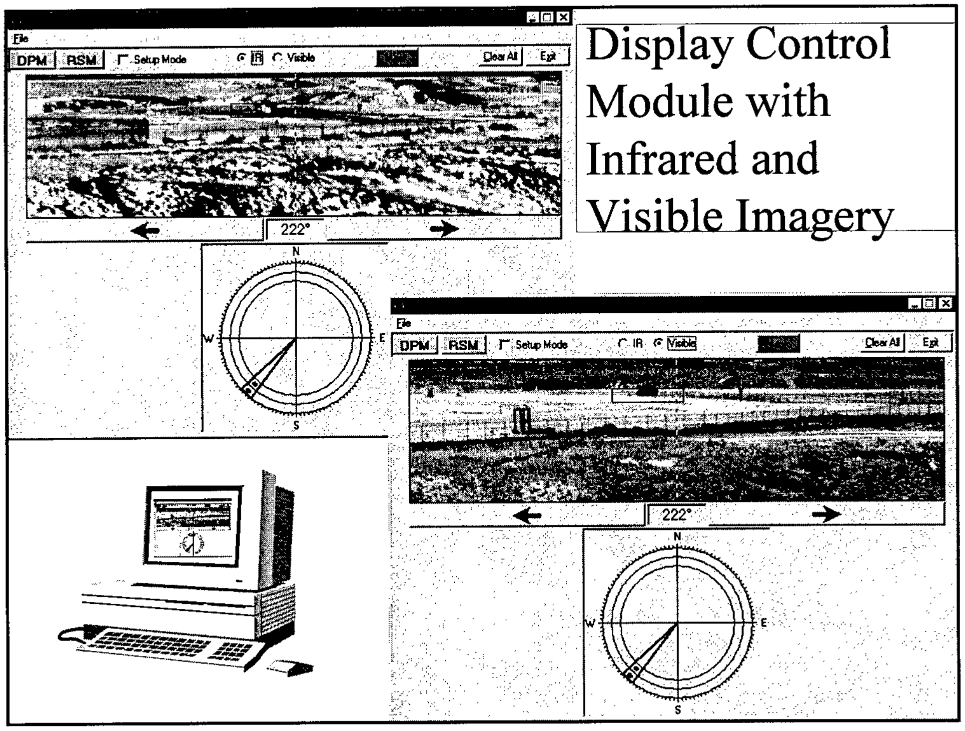
RSM with Cover



Data Processor Module



Display Control Module with Infrared and Visible Imagery



AES Detection "requirements"

- Clear, Good Visibility (day or night) Conditions

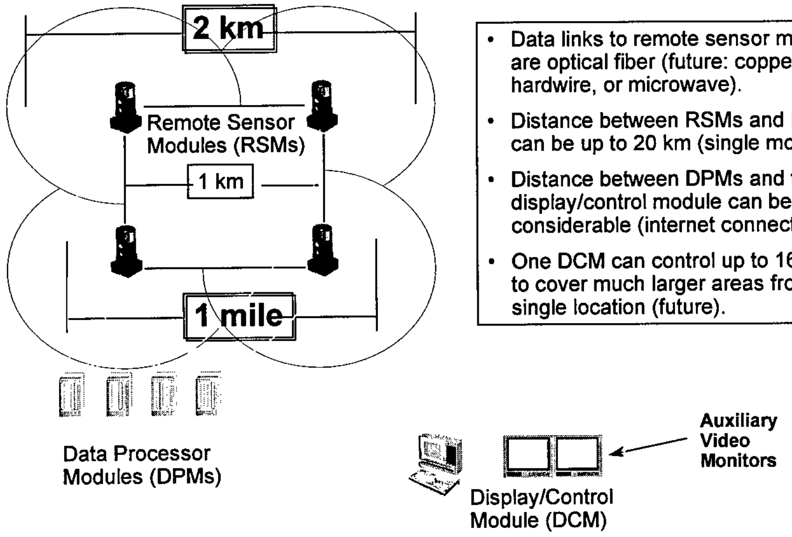
➡Detect walkers / runners at 500 m	(750 m desired)
➡Detect crawlers at 250 m	(375 m desired)
➡Detect vehicles at 1000 m	(1500 m desired)

- Light Rain, Humid Conditions

➡Detect walkers / runners at 350 m	(525 m desired)
➡Detect crawlers at 200 m	(300 m desired)

- Detect as slow as 0.25 m/sec (0.1 m/sec desired)
- Auto re-assess recurring nuisance alarms
  - ➡Continuously track animals once assessed by operator
- Detection to continue while assessing alarms

An AES Application

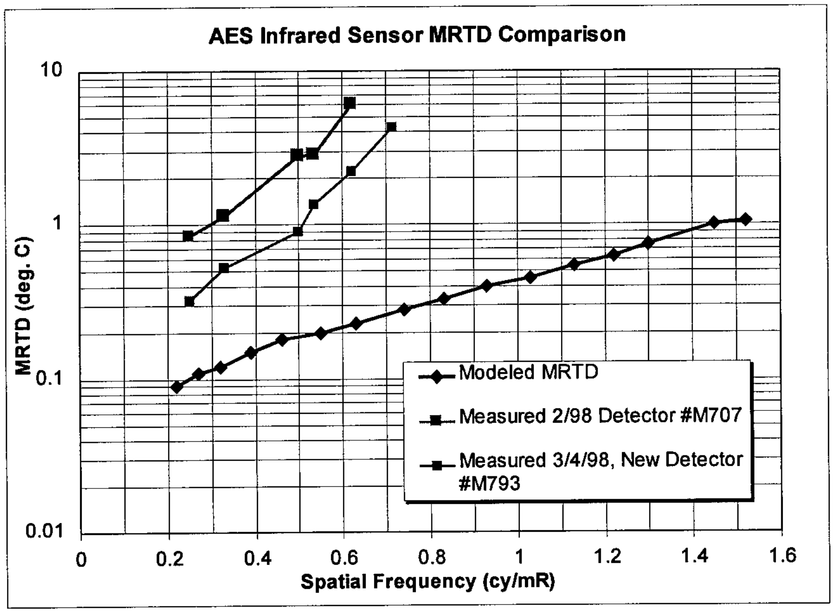

2 km
Remote Sensor Modules (RSMs)
1 km
1 mile
Data Processor Modules (DPMs)
Display/Control Module (DCM)
Auxiliary Video Monitors

- Data links to remote sensor modules are optical fiber (future: copper hardwire, or microwave).
- Distance between RSMs and DPMs can be up to 20 km (single mode fiber).
- Distance between DPMs and the display/control module can be considerable (internet connections).
- One DCM can control up to 16 DPMs to cover much larger areas from a single location (future).

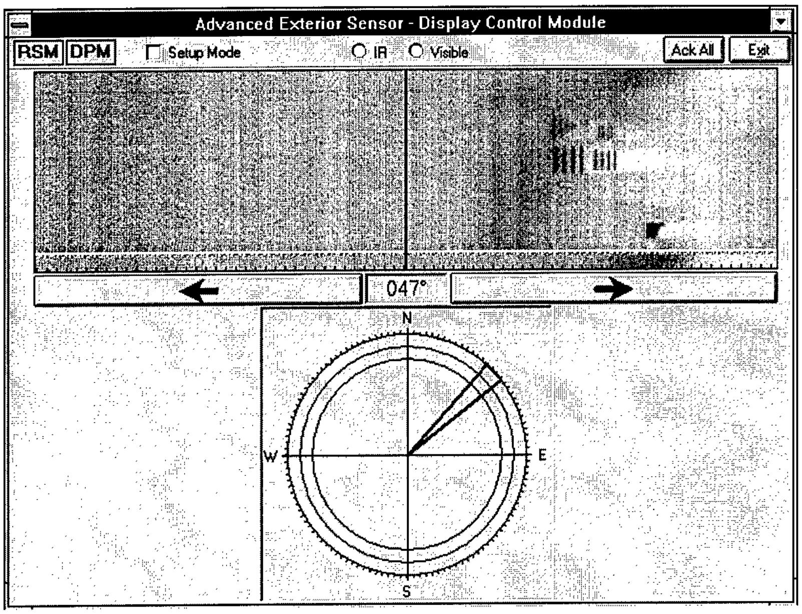
AES Project History

- FY92-93 - Requirements & Technology
  - ➧Determine user's "wants," research emerging technologies, and develop design concept.
- FY94 - Risk Mitigation
  - ➧Model, develop, breadboard, and test software and components to reduce risk and prove technical viability.
  - ➧Develop project plan for development and testing.
- FY95-97 - Prototype Development and Test
  - ➧Prepare for transition to USAF ESC

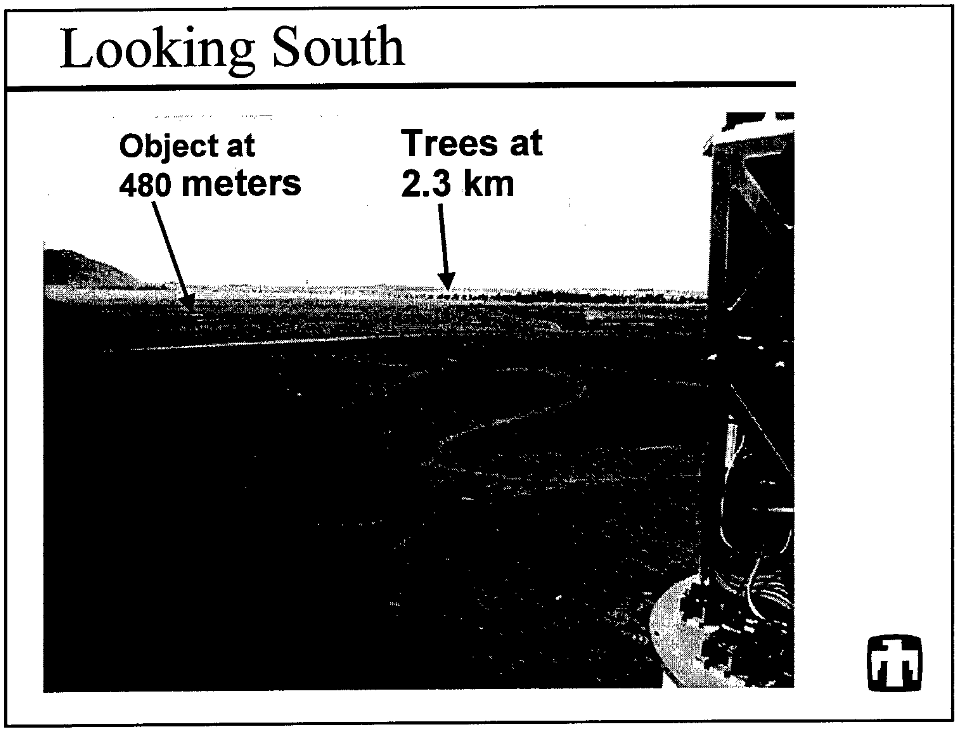
Infrared Sensor Testing Results



MRTD Test Pattern on Display



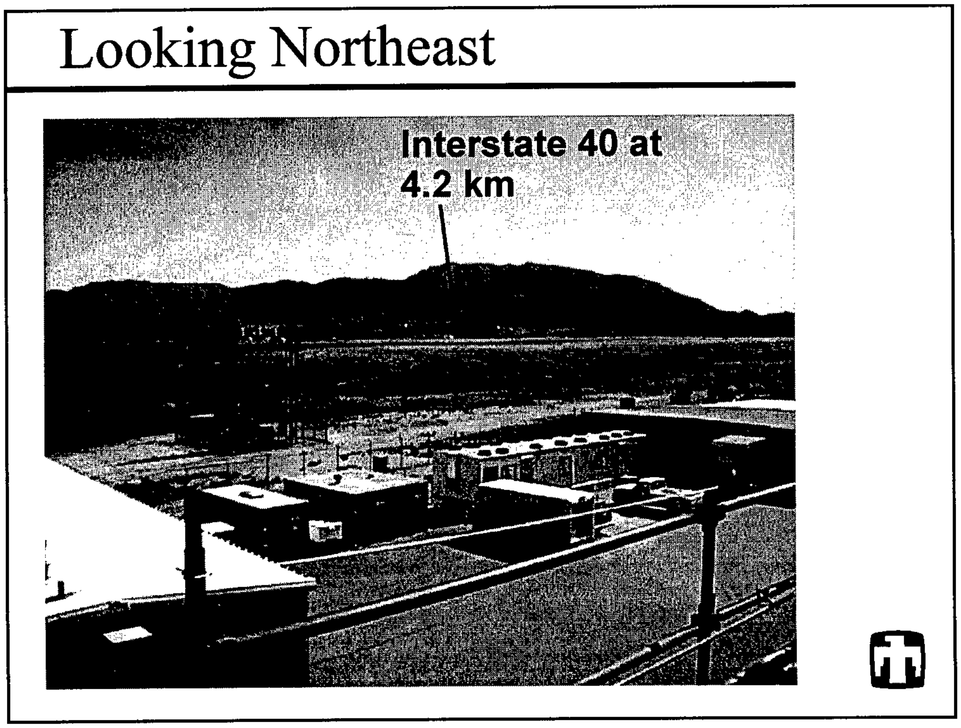
35-Foot Test Tower



Looking South

Object at
480 meters

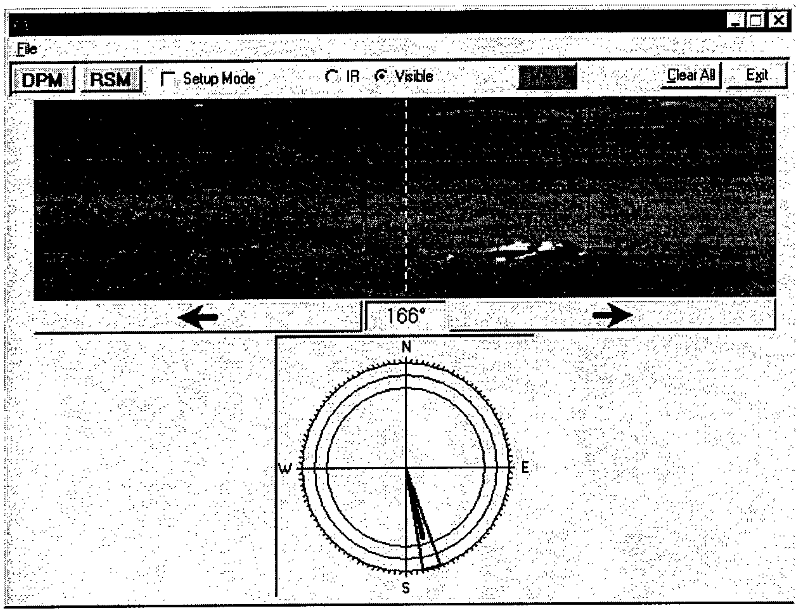
Trees at
2.3 km



Looking Northeast

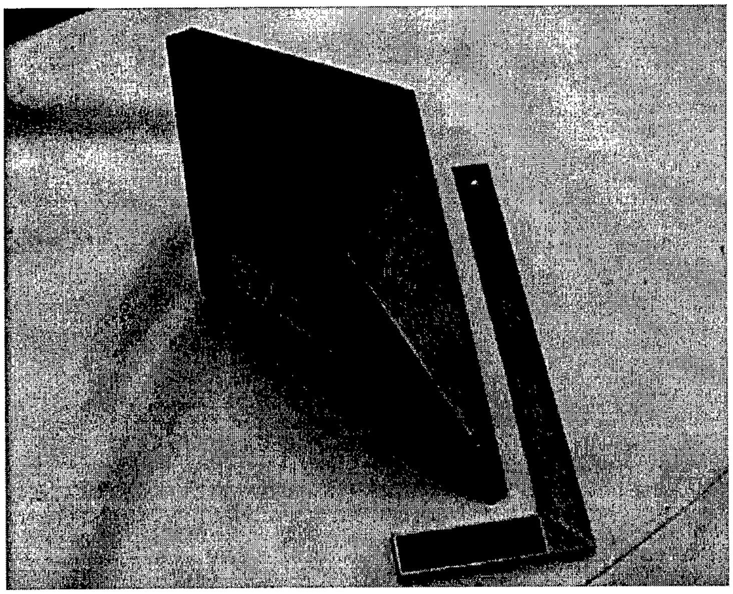
Interstate 40 at
4.2 km

Example of Radar Detection



☐ Setup Mode ○ IR ● Visible

Radar Corner Reflector Test Target



VAMPIRE: Vulnerable Point Protection

Graham Peskett

Session VIII: B Physical Security Technologies

Police Scientific Development Branch
Home Office
Langhurst House
Langhurstwood Road
Horsham
West Sussex
RH12 4WX
United Kingdom

Tel: +44 1403 255451
Fax: +44 1403 213827
Email: gpeskett@langhurst.org.uk

VAMPIRE: Vulnerable Point Protection

Abstract

With the increasing pressure on police manpower and resources, it is important that the correct response is made to each operational call-out. With respect to an alarm from a remote intruder detection system, this is of critical importance. A standard intrusion detection system offers no form of remote verification. Police officers must therefore be deployed in response to the alarm when there is a high probability that it is false. False alarms are a huge drain on police resources. Manufacturers have tried to assist the police by adding audio capabilities to the system. This offers only a small improvement, but with the price of closed circuit television cameras falling, video verification could be the way of the future.

This paper describes VAMPIRE, a Police Scientific Development Branch (PSDB) project which aims to develop a system capable of offering detection in the area surrounding a vulnerable point, combined with remote CCTV verification. At present, most portable detection systems do not have video verification of alarms and are thus not suitable for remote locations. However, by using tried and tested, commercial off-the-shelf technologies we aim to solve the problem in a new and cost effective way.

Such a system has a much wider customer market than remote monitoring of police operations. The armed forces have expensive military hardware that needs protecting. Presently, this guarding is performed by servicemen which again is an expensive use of resources. A VAMPIRE system, as described in this paper, could offer the detection and verification needed.

This paper details the methodology behind and the approach taken to develop a cost effective, vulnerable point, protection system.

Introduction

Policing is a manpower intensive operation and in today's economy where governments are expected to achieve the same quality of results or better with less resources, improving manpower efficiency can achieve a major saving on stretched budgets.

Responding to intruder alarms is only one example of the demands placed on the police service. Calls to alarms caused by weather, equipment malfunction or other non-human activity significantly outnumber calls to genuine intrusions and divert police resources. Staff costs are high so it is important to minimise the frequency of operational call-outs to false alarms. This is particularly important with respect to alarms from a remote detection system. Only 13% of intruder alarm calls received by the police in the UK during 1996 were genuine.

Police forces in the UK operate a 3 level response to an alarm from a remote monitored site. These are:

Level 1: Immediate response;
Level 2: Police response is desirable but attendance may be delayed, eg because of resource availability or higher priority calls; and
Level 3 : No police attendance, keyholder response only.

Initially, all systems are placed on level 1 status. If there are four false calls in 12 months of operation, the police response will move to level 2. Following seven false calls in 12 months level 3 will apply and police response will be withdrawn. The development of technology for reducing false calls by confirming activity within the alarmed premises is endorsed by the Association of Chief Police Officers (ACPO). This is because accurate verification of alarms can increase the effectiveness of the deployment of police officers.

Vulnerable Point Protection

Protecting the entire perimeter of a remote, unmanned site can be expensive. A high calibre fence, intruder detection system, CCTV and additional lighting may all be required to detect successfully and verify an intruder. Even for a small site, the cost of upgrading the existing equipment may be prohibitive. One possible solution is to protect only those objects or areas within the main perimeter that are vital to the operation of the site or are seen as likely targets. These areas are called vulnerable points (VPs). Typically, vulnerable points are moderately small objects or areas in the region of 10m x 20m in size and. It is the external limits of these objects that are protected.

A project was initiated to provide a cost effective solution to the problem of detecting on a short term basis and verifying intruders at VPs on remote unmanned locations. Working to an Operational Requirement (OR) agreed with the customer, PSDB commenced work in Spring 1995 on project VAMPIRE. VAMPIRE is an acronym for Vulnerable Area Methodology for Protection In Restricted Environments.

Initially, the VPs in mind were situated on large, industrial, utility company sites. Such targets included pipes and valves in the oil and gas industries and substations in the electricity industry. The aim was to offer short term detection in the area surrounding these VPs during a period of increased threat. A false alarm rate of 10 or so alarms per system per day was not seen as a major problem as long as the underlying cause of the alarms could be verified.

The requirement was for a system capable of being installed by the technical support units within 4 hours of arrival at site. The maximum time that the equipment was to be deployed on site was estimated at 5 days.

The equipment was to be situated within 3 metres of the VP. Alarm signalling was to be primarily by radio, over a range of 1/2 mile, probably along line of sight. Provision was to be made in the system to use other transmission media such as directly by cable to the response force or by sending the information down a telephone line. It was likely that the area surrounding the VP would be subject to a significant amount of electromagnetic radiation.

Each unit was to be housed in a discreet as possible a container. The system was to be capable of use with a loop framestore storage system. Multiply deployed systems were all to be monitored together at one location, at a maximum of 100 miles from the protected site. The cost of a complete system was not to exceed £3000.

VAMPIRE Solution - Discussion

The basic solution proposed for the system was to combine a number of detectors with CCTV cameras such that when an intrusion occurred at a zone the pictures from the camera observing the zone were transmitted to a remote location for verification.

Designing a new sensor would require a substantial amount of investment and would increase the timescales of the project. It was therefore decided to use commercial off-the-shelf technologies. One significant advantage of this approach is that all the individual components had been tried and tested and found to be reliable in operation.

Several types of detectors were considered and their merits and weaknesses evaluated. Passive infra red (PIR) sensors were chosen because of their efficient operation and high detection performance. The chosen PIR detectors had a corridor curtain detection pattern, operating over a range of 0-30m. This was achieved by using mirror optics to focus the infra red radiation onto the pyrosensor. Many other PIR designs were considered but most of them offered a volumetric detection pattern over a wide angle. The external detectors which were evaluated, operated over a much longer distance with the detection curtain starting after several metres. This initial region, ie from 0m to 30m from the detector is precisely the range in which we were looking to detect an intruder and therefore these sensors were deemed unsuitable.

Eight of the selected PIRs were linked in pairs to form a rectangular perimeter surrounding the vulnerable point. By using simple logic circuits, the two opposing detectors observing the same side of the rectangle were ANDed together such that an alarm needed to be signalled by both detectors simultaneously before a main alarm event was triggered. This created four separate zones. A time window could be included such that an alarm could be received from either sensor within a given period and a main event be signalled.

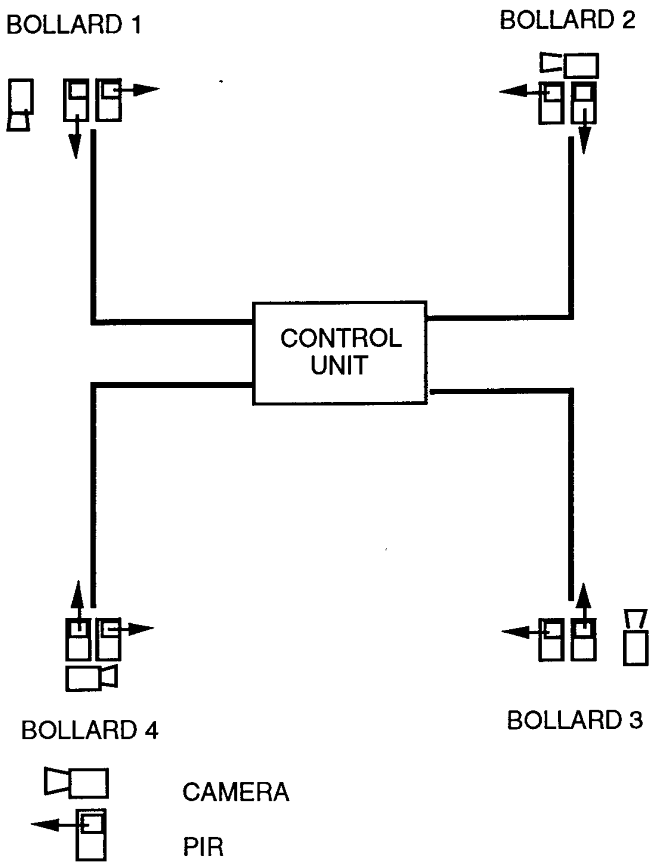


Figure 1: Schematic of the prototype VAMPIRE

A problem associated with PIR sensors is defining the exact range of the detector. By combining pairs of sensors in this way the zone length was tightly defined as being between the two sensors, even though each sensor could detect past its counterpart. This created a simple beam-break system, similar to a pair of active infra red detectors. The alignment of active infrared systems is, however, critical to achieve effective operation. With a passive based system the detection curtain is wider and therefore the alignment is less critical. This makes the system easier to deploy operationally.

Audio verification of alarms requires a well trained ear to establish whether the alarm is likely to be true or not. Visual verification can often achieve improved results.

Each pair of PIRs had a monochrome printed circuit board camera associated with it. The Operational Requirement did not call for broadcast quality, high resolution images. It would be sufficient to use cameras with adequate detail to enable an operator to determine whether an intruder was in the scene. Because of the short distances to be covered by the system, the cameras had short focal length lenses fitted. It followed that the target would occupy a large percentage of the TV monitor screen height, thus aiding the operator to determine the cause of the alarm.

When a main alarm event was detected, the camera observing the zone of the intrusion would be switched and the pictures associated with the alarm would be transmitted to a remote operator for verification.

The areas where the system was likely to be installed had sufficient ambient light levels for use with the cameras and additional illumination was not therefore required. Because of the relatively short lengths of the detection zones, infrared LED illumination has been considered as a possible solution, should additional lighting be required. Lighting of this nature means low power consumption, low heat emission and that the system is more covert than one which uses a white light source.

VAMPIRE -Prototype

A prototype system was constructed by mounting the sensors, together with the cameras, inside plastic tubing with a 130mm inner diameter, at a height of 1.35 m. The video switchgear and transmission equipment was housed in a separate unit. The construction cost for the prototype was approximately £3500.

The transmission of the alarm images was achieved by using a UK license exempt radio frequency transmitter. This system was capable of transmitting real time images over a distance of 750m line of sight. If the monitoring station was located further away then the pictures from the RF receiver unit could be fed into a remote telephone transmission system housed in a convenient building. The 750m distance was considered far enough to ensure that the necessary telephone connections would be accessible.

The prototype system was installed at our rough weather testing site to monitor the performance. The system was used for the protection of a zone equivalent to one side of length 25 metres of an area enclosing a vulnerable point. Each individual sensor was monitored, and by using statistical techniques it was possible establish a suitable time window for effective operation. The initial monitoring period of 3 months has shown a low average level of false alarms. Data analysis indicates that this figure could be as low as 1 false alarm per zone per day.

Customer Impressions

The PSDB prototype system has been demonstrated to many potential customers and has attracted a significant amount of interest. Although the prototype did not meet all potential customer needs, it would be possible to produce a system to meet other specific requirements. The sensor heads, with their combined detection and verification have attracted the most interest. Some suggestions for modifications have been incorporated in to the development system. However, it would be impractical to try and address the needs of all customers in one system.

By making the production units in a modular design, it may be possible to vary the number of detectors and cameras and the type of transmission system to fulfil particular requirements.

The technology developed in this project is not restricted to the protection of commercial vulnerable points. Other possible applications are to protect military hardware when deployed operationally, ie in UN peacekeeping detachments.

A pre-production system is currently under construction and will be installed at an operational site.

Future Technologies

Some police investigations require officers to mount a surveillance operation. A covert VAMPIRE system could be used to protect officers deployed in observation posts. The development of small sensor heads with remote transmission of both alarm and video, could provide aid in these situations. Such miniature sensor heads could be placed in suitable hides.

It may be possible to incorporate some basic form of video motion detection in the system to filter out false alarms. This would operate along similar lines to an AMETHYST system (1)

Other technologies are constantly being developed. Cameras with built in memory devices could be incorporated to allow the recording of pre- and post- alarm pictures. When played in sequence a loop of images so recorded could aid verification.

Conclusion

With the constant demand for a more efficient use of law enforcement resources and the price of CCTV cameras falling, the use of video verification of alarms is set to increase. VAMPIRE provides a possible solution for the protection of vulnerable points.

References

1 Horner M.
Police Scientific Development Branch
29th Annual International Conference on Security Technology (1995)
AMETHYST: An Enhanced Detection System Intelligently Combining Video Detection and Non-Video Detection Systems.

14th Annual NDIA Security Technology Symposium

June 15 - 18, 1998

Information System Vulnerabilities

Mark Fabro

International Director, Assessment Services

Secure Computing Corporation

NDIA
NATIONAL DEFENSE INDUSTRIAL ASSOCIATION

SECURE
COMPUTING

SECURE
COMPUTING
Nobody Comes Close

Agenda

NDIA

- **Some Vulnerabilities**
- **Questions**

7/17/98

SECURE
COMPUTING
Nobody Comes Close

Denial of Service

NDIA

- Ghost Routing (LAND), smurfing, teardrop, boink
- SYN Sniping (reset killing)
- Webserver DoS (Apache, IIS - rewrite access list)
- SYN flooding (Neptune, flood)
- Data/Service bombs (UDP, ICMP, finger)
- Service loops (chargen, echo), NTWINS
- OS specific bombing (time, memory leaks)
- High port overflows; server fills (routed, syslog)
- Hostile Applets (Ungr8ful, Downtime)
- Mailbombing (UpYours, Avalanche, Unibomber, DnD)

7/17/98

SECURE
COMPUTING
Nobody Comes Close

The Web Servers

- Severs running OTHER services beyond httpd
- Forms/scripts - ‘phf’,‘php’,‘campus’, ‘handler’ exploits (NCSA/Apache)
- counter exploits and cgi-bin test scripts
- True directory listings
- *Domino* - link redirection
- *Uploader.exe* (O’Reilly)
- modifications to ‘.htaccess’ if attacker has ftp access
- Web spoofing redirects; hidden files (HFF)

7/17/98

Packet Fragmentation

- Widely available tools/easy to use
- Manipulation of reassembly techniques at target
- Blows past anything that allows fragmented packets
- Partial solution in RFC 1858
- NT(pre SP3) through PF firewalls

7/17/98

SECURE
COMPUTING
Nobody Comes Close

FTP bouncing / core dumping

NDIA

- Manipulate ftp PASV mode
- Use PORT and QUOTE to send scripts
- Gain access to unauthorized ftp sites
- Looks legitimate
- Similar methods used for untraceable mail, news
- Fill servers, hop firewalls
- other versions use PORT to make calls to internal
- Exploit authentication mechanism
- Force pwd file to core
- Some ftp servers host '.rhosts' file

7/10/98

SECURE
COMPUTING
Nobody Comes Close

War Dialing

- Non-sequential dialing of area prefixes
- ‘WELCOME’ messages and login help
- People assume being unpublished is safe
- WAR/Demon dialers are being developed
- TonLoc / PhoneTag / A-dialer / Z-hacker
- Access networks through dial-in
- Advanced to beat tracking and tracing
- see Shipley (1997)

7/17/98

DNS Exploits

- Forged UDP packets can corrupt BIND/WinNT nameserver caches
- Based on servers handling recursive queries
- Add an 'A' record to the DNS of *victim.com* to resolve *www.anotherhost.com* to 127.0.0.1
- Capturing *dns.victim.com* packets to *dns.attacker.com* allows retreival of **qid0 (query ID)** of *dns.victim.com*
- Send query to *dns.victim.com* asking for *www.anotherhost.com* using next qid
- Flood *dns.victim.com* with spoofed replies from *dns.anotherhost.com* saying that *www.anotherhost.com is 127.0.0.1 (or whatever)*

7/17/98

Others

- Broken (config) Firewall - ACK storm, SYNACK flood
- Buffer overflow attacks
- Plaintext sniffing (hijacking)
- Social Engineering
- NT (broken) on external
- Bad network config (NAT)
- Protocol tunneling

Many, many, many more

7/17/98

The Challenge

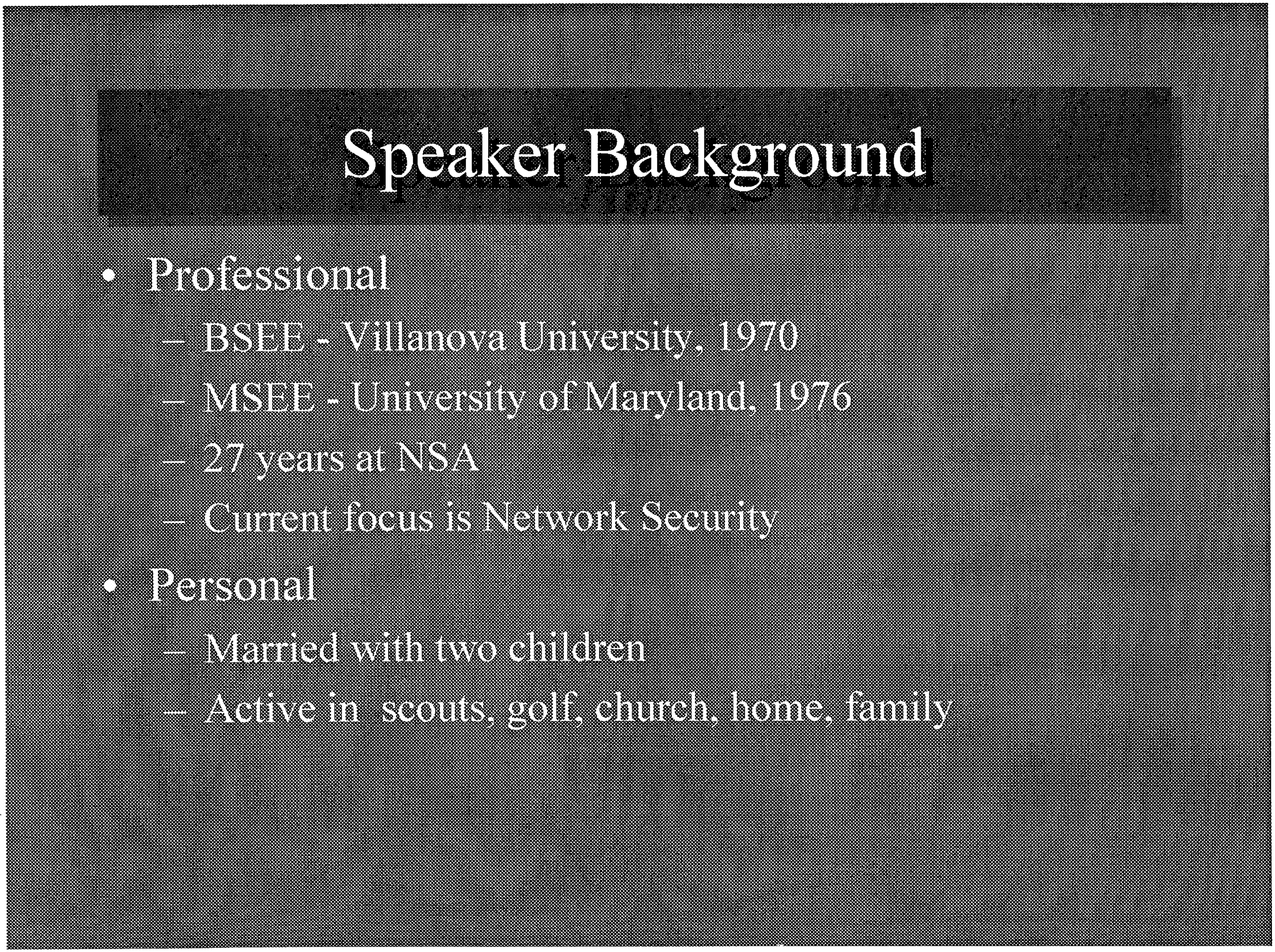
- Learning the threats
- Learning where you are vulnerable
- Assess your weakness
- Show upper managers ($$$)
- CONVINCE upper managers
- Countermeasure application
- Reasses
- Try and keep up....

7/17/98

Network Security Framework

National Defense Industrial Association
18 June 1998

David E. Luddy
NSA - X1 Technical Director
Network Security Group, Systems Engineering Office
deluddy@missi.ncsc.mil

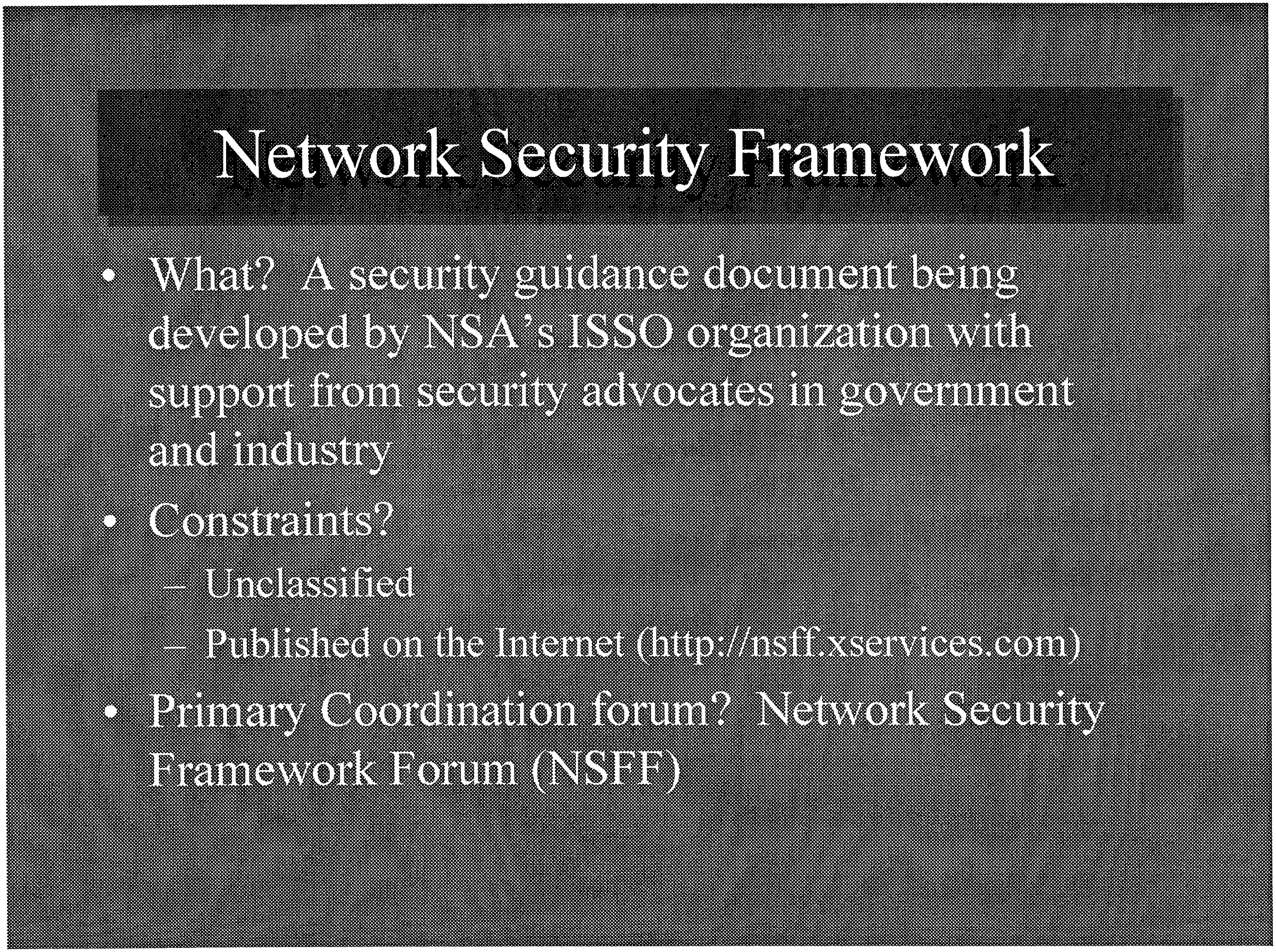


Speaker Background

- Professional
  - BSEE - Villanova University, 1970
  - MSEE - University of Maryland, 1976
  - 27 years at NSA
  - Current focus is Network Security
- Personal
  - Married with two children
  - Active in scouts, golf, church, home, family

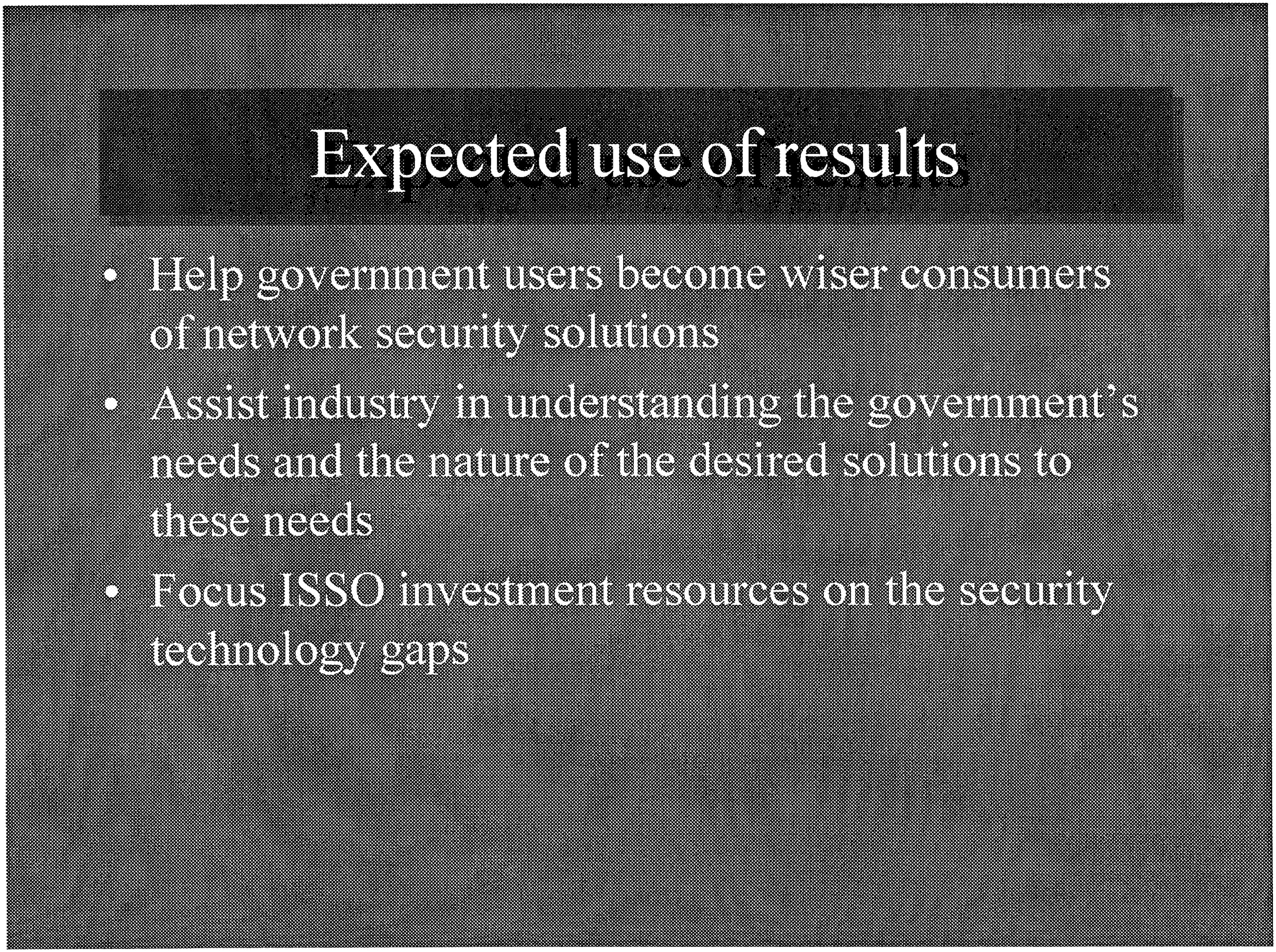
Purpose of Briefing

- To provide the focus and highlights of two Information Assurance Initiatives:
  - Network Security Framework
  - Network Security Framework Forum



Network Security Framework

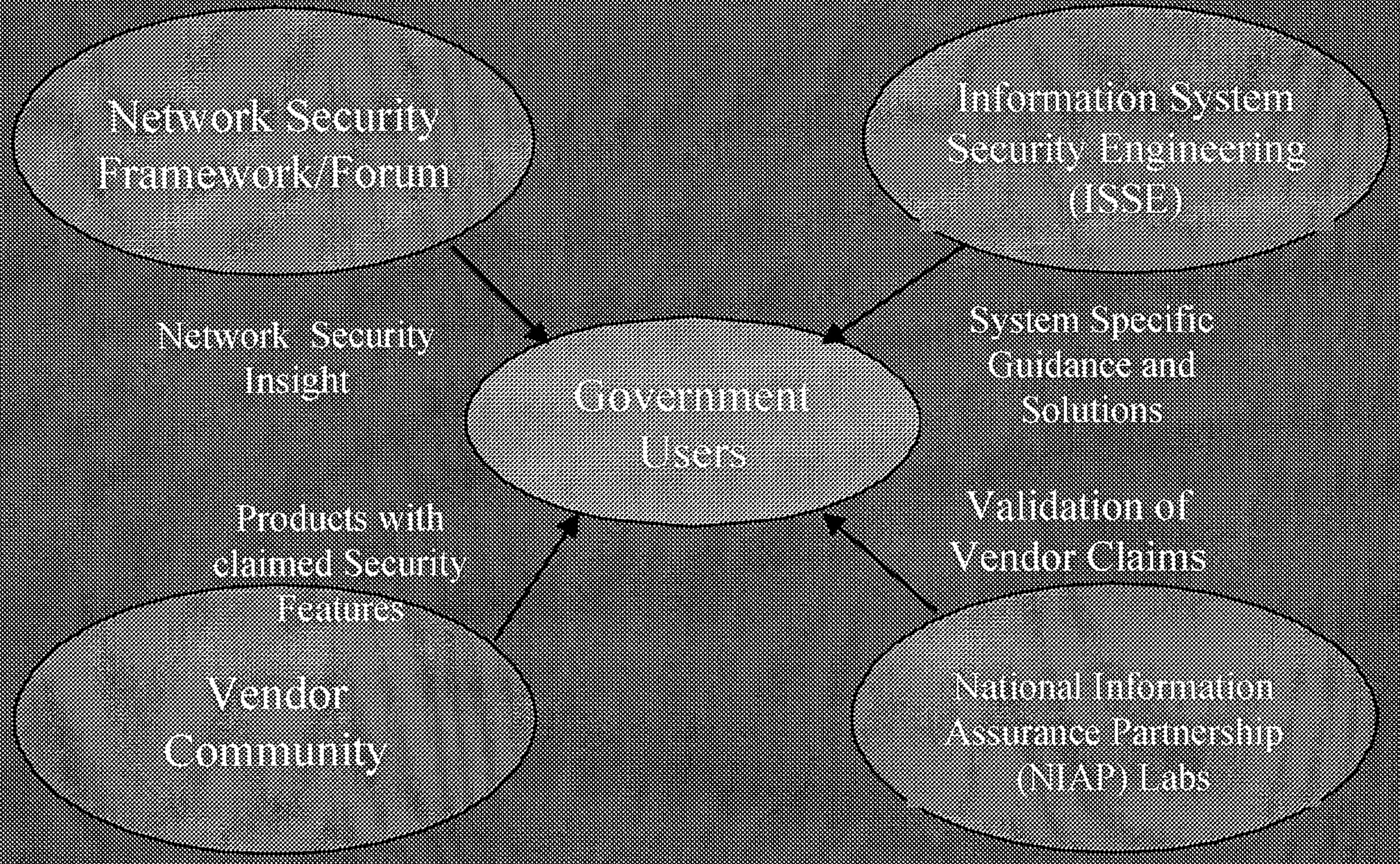
- What? A security guidance document being developed by NSA's ISSO organization with support from security advocates in government and industry
- Constraints?
  - Unclassified
  - Published on the Internet (http://nsff.xservices.com)
- Primary Coordination forum? Network Security Framework Forum (NSFF)



Expected use of results

- Help government users become wiser consumers of network security solutions
- Assist industry in understanding the government's needs and the nature of the desired solutions to these needs
- Focus ISSO investment resources on the security technology gaps

Relationship to other Information Assurance Initiatives

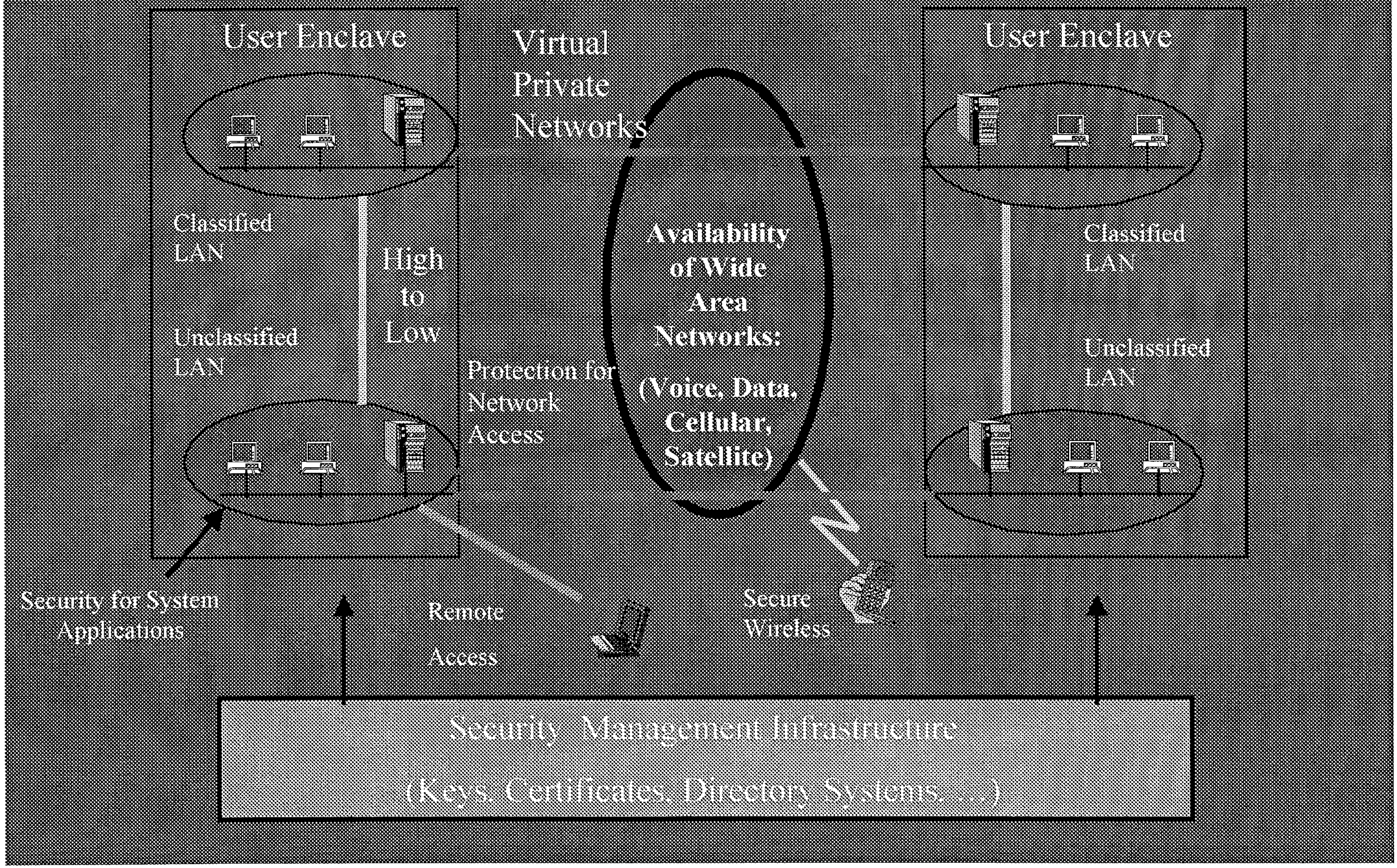


Network Security Framework/Forum
Information System Security Engineering (ISSE)
Network Security Insight
Government Users
System Specific Guidance and Solutions
Products with claimed Security Features
Validation of Vendor Claims
Vendor Community
National Information Assurance Partnership (NIAP) Labs

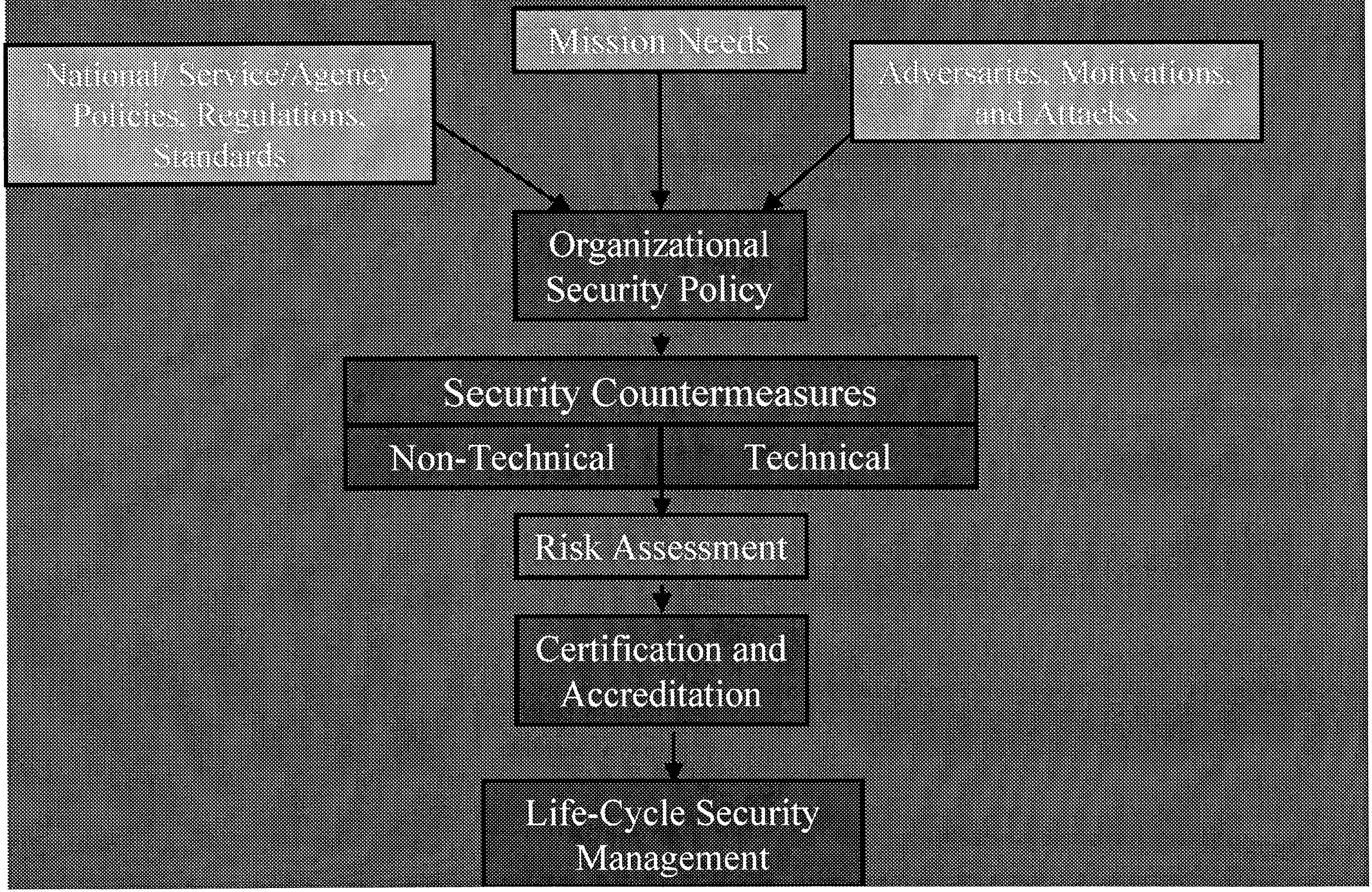
Primary topics addressed in the Network Security Framework

- Characterization of Customer Needs
- Security Methodology
- Classes of Attacks
- Technical Security Principles
- Security Solution Guidance
- Security Management Infrastructure

Security Focus Areas


User Enclave
Classified LAN
Unclassified LAN
High to Low
Virtual Private Networks
Protection for Network Access
Availability of Wide Area Networks: (Voice, Data, Cellular, Satellite)
User Enclave
Classified LAN
Unclassified LAN
Security for System Applications
Remote Access
Secure Wireless
Security Management Infrastructure
(Keys, Certificates, Directory Systems, . . .)

Security Methodology



National/ Service/Agency Policies, Regulations, Standards

Mission Needs

Adversaries, Motivations, and Attacks

Organizational Security Policy

Security Countermeasures

Non-Technical

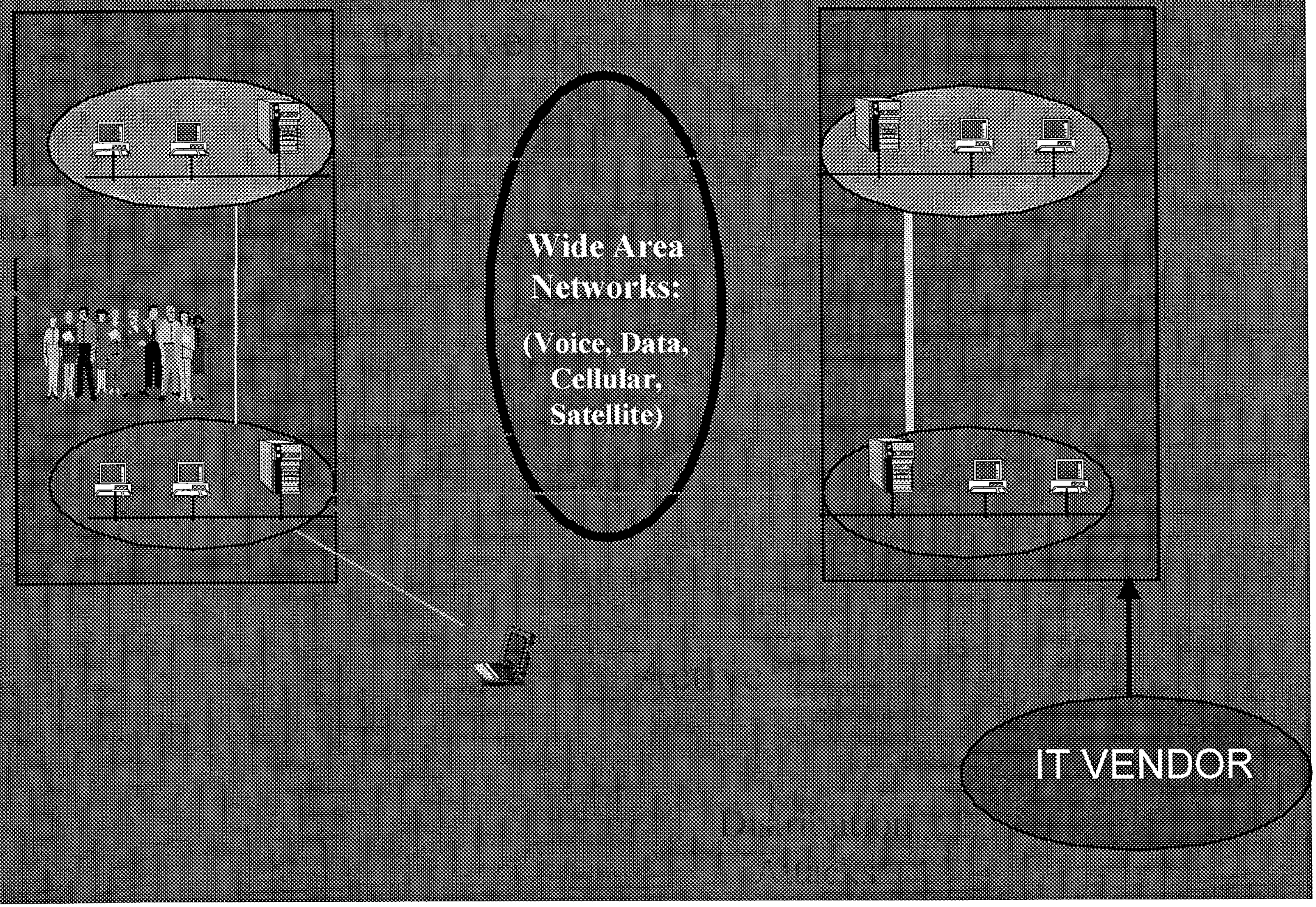
Technical

Risk Assessment

Certification and Accreditation

Life-Cycle Security Management

Classes of Attacks



Robustness Strategy

- Purpose: To help using organizations answer this question, "What strength and assurance levels are needed for solutions to particular problems"
- Recommended approach.
  - Define the Value of the Information/Network being protected
  - Assess the Threat
  - Find recommend Strength and Assurance Levels in the framework
  - Procure and Test solutions that provide the achieve these levels

NSF Robustness Strategy

Threat Levels

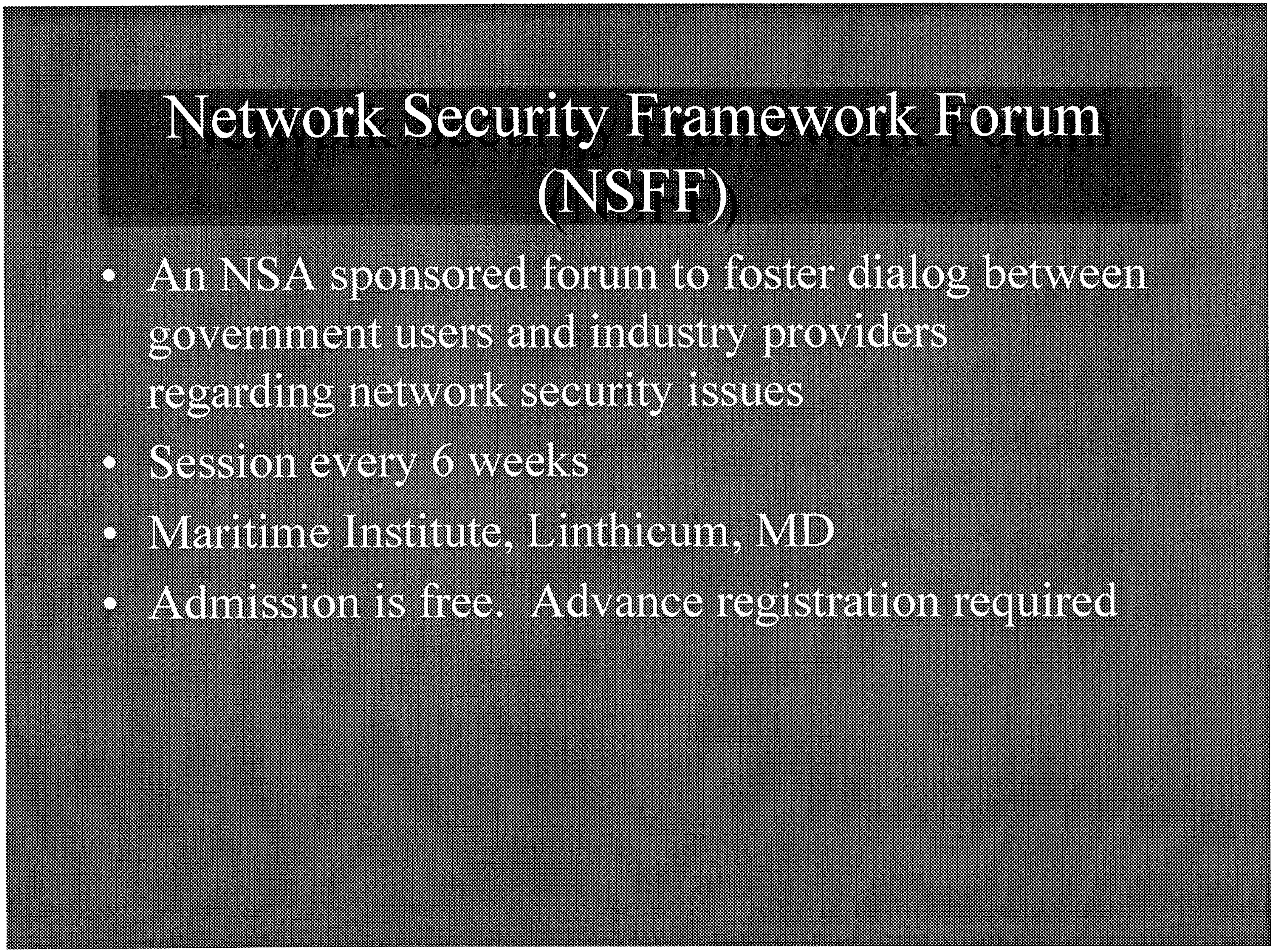
	T1	T2	T3	T4	T5	T6	T7
V1	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML1 EAL2	SML1 EAL2
V2	SML1 EAL1	SML1 EAL1	SML1 EAL1	[illegible]	[illegible]	[illegible]	[illegible]
V3	SML1 EAL1	SML1 EAL2	SML1 EAL2	[illegible]	[illegible]	[illegible]	[illegible]
V4	[illegible]	[illegible]	[illegible]	SML3 EAL5	SML3 EAL5	SML3 EAL6	SML3 EAL6
V5	[illegible]	[illegible]	SML3 EAL4	SML3 EAL5	SML3 EAL3	SML3 EAL6	SML3 EAL7

Security Solution Framework

- Topics addressed for each category
  - Consolidated user requirements
    - Known
    - Emerging
  - Applicable attacks
  - Generic Security countermeasures
  - Security technology assessment
  - Requirements cases
  - Case specific guidance
    - Desired solution
    - Best of breed solution

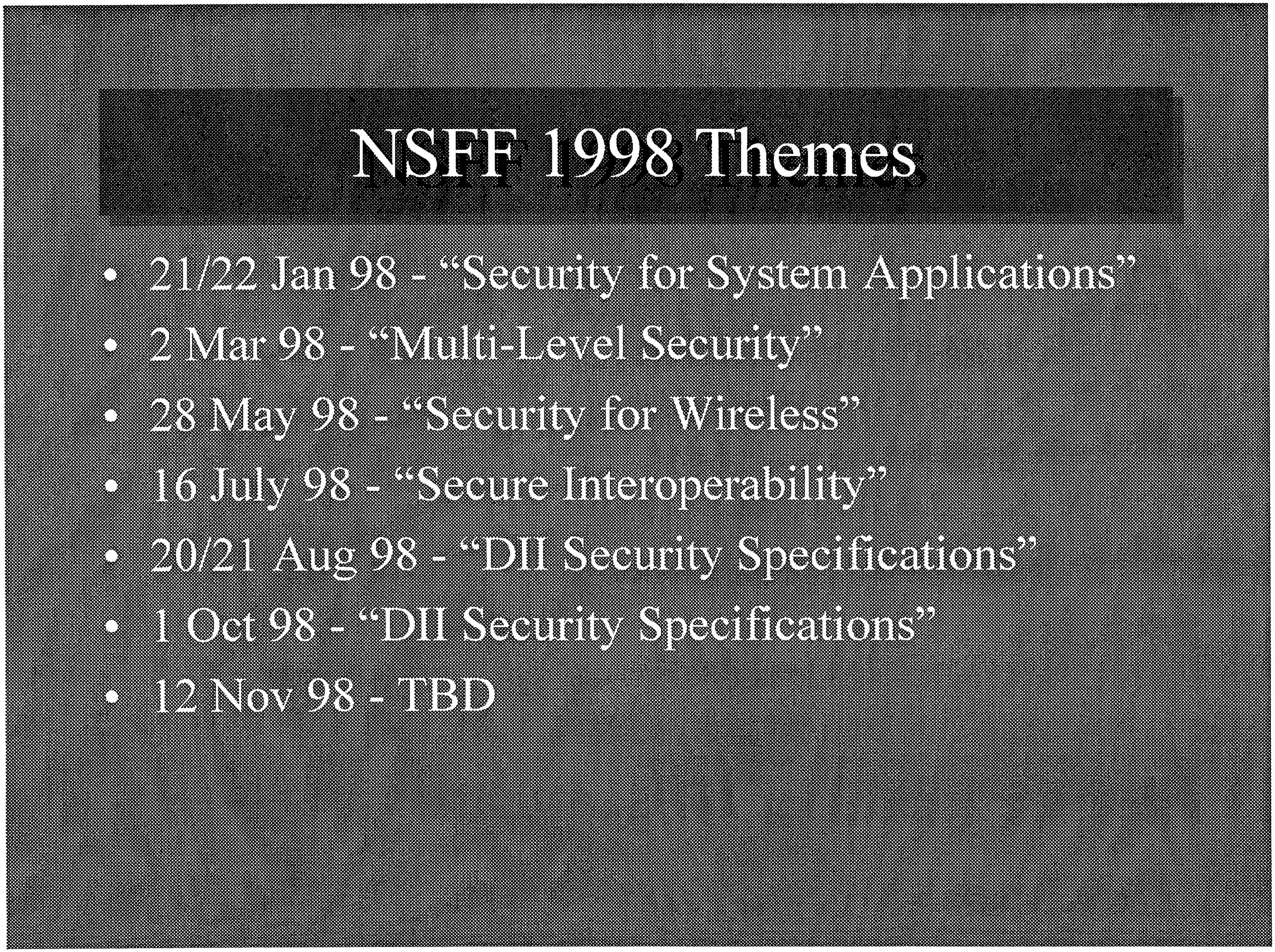
Nature of Case Specific Guidance

- Identify Primary Security Components (Functional)
- For each component
  - – Security Features
  - – Security Strengths
  - – Security Assurance
    - Common Criteria Level (EAL 1-7)
  - – Interoperability
  - – PKI features and assurance (Levels x, y,z)



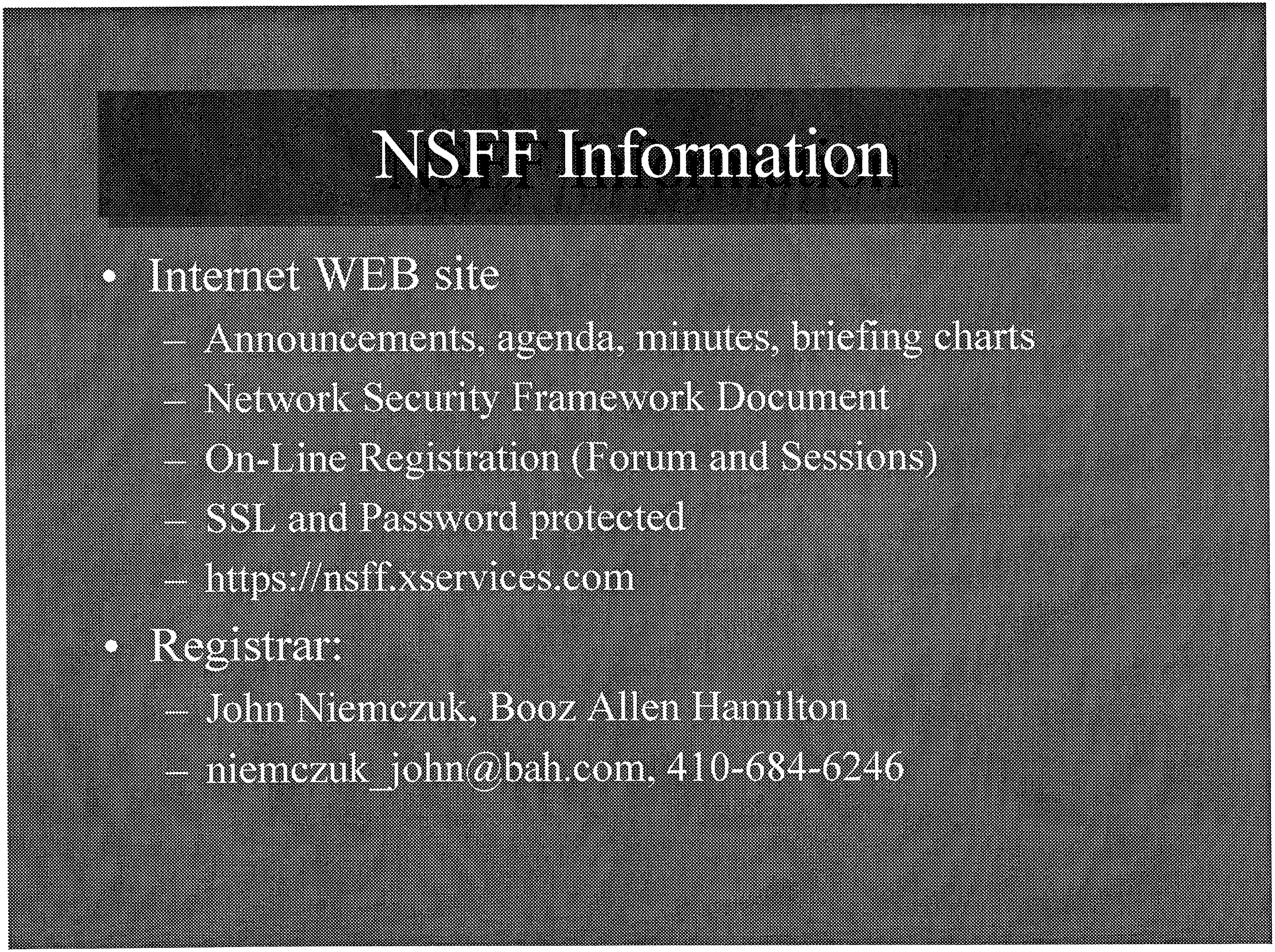
Network Security Framework Forum (NSFF)

- An NSA sponsored forum to foster dialog between government users and industry providers regarding network security issues
- Session every 6 weeks
- Maritime Institute, Linthicum, MD
- Admission is free. Advance registration required



NSFF 1998 Themes

- 21/22 Jan 98 - "Security for System Applications"
- 2 Mar 98 - "Multi-Level Security"
- 28 May 98 - "Security for Wireless"
- 16 July 98 - "Secure Interoperability"
- 20/21 Aug 98 - "DII Security Specifications"
- 1 Oct 98 - "DII Security Specifications"
- 12 Nov 98 - TBD



NSFF Information

- Internet WEB site
  - – Announcements, agenda, minutes, briefing charts
  - – Network Security Framework Document
  - – On-Line Registration (Forum and Sessions)
  - – SSL and Password protected
  - – https://nsff.xservices.com
- Registrar:
  - – John Niemczuk, Booz Allen Hamilton
  - – niemczuk_john@bah.com, 410-684-6246

Introductory Remarks
Session X. The Resources: Are There Enough?

Brigadier General Roger C. Smith, USAF (Ret.)
Session Chair

We have kept the most difficult issues for last. Earlier in the Symposium we discussed the changing nature of the threat and the planned responses outlined in Presidential Decision Directives 62 and 63. We have also heard in some detail about the findings of the President's Commission on Critical Infrastructure Protection, which explored the growing vulnerability of the nation's infrastructure. The Joint Chiefs, responding to the terrorist action at Khobar Towers, have established a new directorate for Combating Terrorism, J-34, and we had the opportunity to hear Brigadier General Conway discuss the new emphasis on force protection and counterterrorism initiatives.

But to the average American, the United States is at peace in the world. Another military action against Iraq has been avoided. U.S. forces are deployed overseas, but the focus is on peacekeeping and humanitarian actions. At home, the average American sees a period of relative prosperity; there are projections of a five-year federal budget surplus, and continued reductions in the Department of Defense budget.

These economic and social trends seem to be inconsistent with much of what we have discussed over the past two days. Many Americans seem unconcerned about the growing vulnerability of elements of our national and economic security. A rising threat of terrorism at home and abroad receives little attention as the Khobar Towers, Oklahoma City and World Trade Center events fade into memory. Many Americans would be reluctant to accept additional security and protection measures in their daily lives unless and until they directly experience an untoward event.

This final session will address these inconsistencies and other questions basic to the resources issue. Given the current economic and social environment, will there be adequate federal government funding and resources to provide the levels of protection and security required to preserve our economic, military and national security? How do these needs stack up with other national priorities, and are they holding their own in the national debate? Are policy makers sufficiently concerned to make the difficult budget decisions?

Our guest speakers this morning need little introduction. We are very fortunate to have them share with us their valuable perspectives on these issues.

Tim Sample is the Deputy Staff Director of the Permanent Select Committee on Intelligence, U.S. House of Representatives.

Peggy Evans is the Chief, Command, Control, Communications and Intelligence, Office of Management and Budget, Executive Office of the President.

Closing Remarks

Brigadier General Roger C. Smith, USAF (Ret.)
Chairman, Security Division

This concludes our 14th annual Security Symposium. I hope that we have provided some fresh insights into the new dimensions of security, both in terms of emerging threats and promising countermeasures.

We have sought to explore how security technology fits into the overall picture of broader security concerns. We have offered some new perspectives on the interdependency of all the elements of security in dealing with a more challenging, diverse domestic and international environment.

We have addressed the role of security forces and technical capabilities as key weapons in preventing, detecting, responding to, mitigating, and recovering from both conventional and unconventional physical and cyber attacks.

A major question we face now is how to implement the findings of this symposium. A year from now, we should ask ourselves what actions have been taken to integrate changing security and protection principles and new technologies into the overall security equation.

We look forward to having you attend the 15th Annual Security Symposium, on 14-17 June of next year, in beautiful Norfolk, Virginia. Thank you for attending. Have a safe trip home and a productive year.